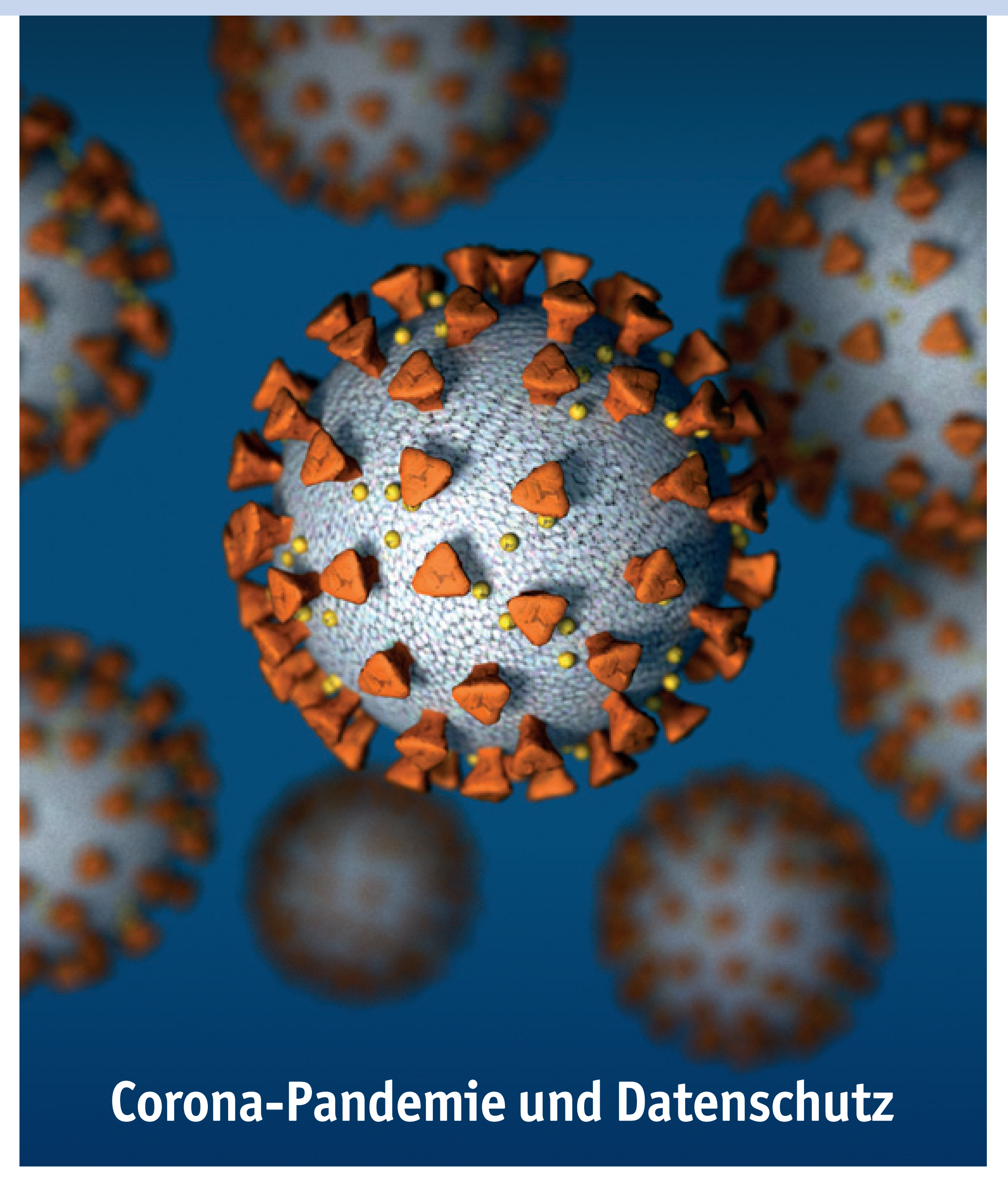
2/2020

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

43. Jahrgang
ISSN 0137-7767
14,00 Euro



Corona-Pandemie und Datenschutz

■ Mit digitaler Technik gegen die Pandemie ■ Tracing-Apps datenschutzfreundlich gestalten ■ Videokonferenz-Software ■ Corona-Nachrichten ■ Handydaten zur Eindämmung des Coronavirus? ■ Pressemitteilungen ■ E-Payment in Taiwan ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Foto: Pixabay..com

Samstag, 01. August 2020
Redaktionsschluss DANA 3/2020

Montag, 14. September 2020
Sommerakademie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein
Kiel

Freitag, 18. September 2020
BigBrotherAwards
Stadttheater Bielefeld

DANA
Datenschutz Nachrichten
ISSN 0137-7767
43. Jahrgang, Heft 2

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Dr. Thilo Weichert
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

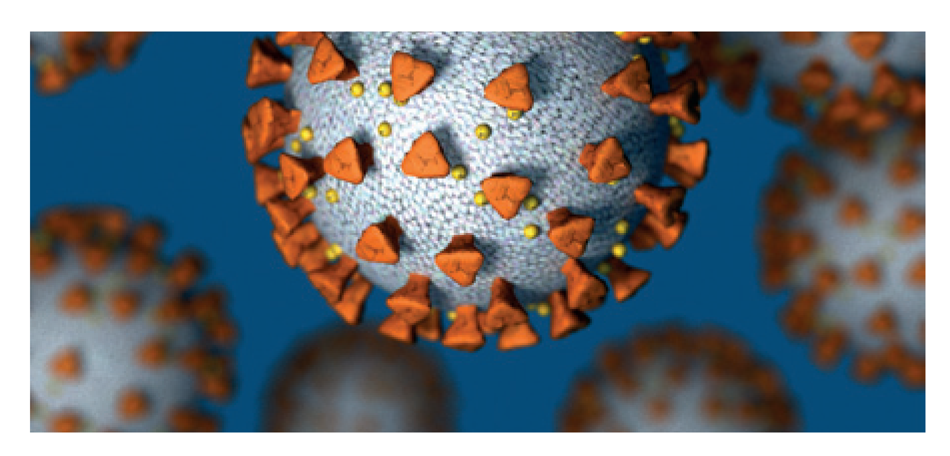
Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta,
Pixabay, iStock

Editorial



Langfristig war geplant, dass sich das vorliegende Heft 2 der Datenschutz Nachrichten mit elektronischen Zahlungssystemen und deren Relevanz für den Schutz von Privatheit und Grundrechten befasst. Doch ist die Aktualität der Corona-Pandemie dazwischen gekommen: Die Diskussion über die Frage, was zur Eindämmung des Virus nötig ist, insbesondere wenn dadurch Grundrechte betroffen sind, macht vor dem Grundrecht auf Datenschutz nicht halt.

Corona-Apps, Datenspende-Apps, fragwürdige Datenübermittlungen und mehr haben mit dem Virus plötzlich das Thema Datenschutz in den gesellschaftlichen Vordergrund gepusht. Dabei führt die Globalität der Gesundheitsbedrohung fast zwangsläufig dazu, das Thema weltweit in den Blick zu nehmen. Hierbei sticht der Systemgegensatz zwischen Europa und China hervor, der unter dem Brennglas der Coronabekämpfung besonders gut zu erkennen ist, und der zugleich klarmacht, welche globale Aufgabe dem europäischen Datenschutz zukommt. Verblüffend und erfreulich ist, dass sich – zumindest zum Zeitpunkt des Redaktionsschlusses dieses Heftes (Ende April) – vernunft- und grundrechtsorientierte Politik in weiten Teilen Europas durchzusetzen scheint.

Es bleiben viele weitere Themen auf der Tagesordnung. Diese haben teilweise eng mit der Corona-Pandemie zu tun, etwa wenn sich wegen körperlicher Kontaktverbote digitale Videokontaktangebote geradezu aufzwängen. Corona ist nicht alles, weshalb insbesondere im Service- und Nachrichtenteil weitere aktuelle Fragestellungen – und auch dies weltweit – behandelt werden. Einen Blick in die Welt der Zahlungssysteme gibt Frau Prof. Wu mit ihrer Darstellung des E-Payment in Taiwan.

Die DANA-Redaktion

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder
Vorstandsmitglied in der DVD,
alenfelder@datenschutzverein.de, Köln

Kirsten Bock, Christian Ricardo Kühne, Rainer Mühlhoff, Mĕto R. Ost, Jörg Pohle, Rainer Rehak
WissenschaftlerInnen und DatenschützerInnen im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V., dsfa-corona@fiff.de

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Prof. Shu-Ru Wu
Department of Law, Chinese Culture University, Taipei
rechtswissenschaft@hotmail.com, https://law.pccu.edu.tw/bin/home.php

Thilo Weichert

Mit digitaler Technik gegen die Pandemie – mit oder ohne Bürgerrechte? –

1 Einleitung

Im Zeitalter des Smartphones ist die Ansicht weit verbreitet, mit Hilfe dieses digitalen Wunderdings ließe sich irgendwie fast jedes Problem lösen. Angesichts der aktuellen Corona-Pandemie scheint es so naheliegend, das Smartphone gegen diese globale Gesundheitsgefahr zum Einsatz zu bringen. Informationstechnik kann nicht das Virus vertreiben. Viele hoffen aber, mit ihr das vom Coronavirus (SARS-CoV-2) ausgehende Risiko für die Menschen zu beschränken und dessen Ausbreitung einzuschränken. Dass dies nicht abwegig ist, wurde in China oder in Südkorea gezeigt, wo digitale Überwachung einen Beitrag dazu leistet, die Ausbreitung des Virus einzuschränken. Damit steht die Frage im Raum: Was bringt was? Und inwieweit ist der Einsatz solcher Instrumente mit Grundrechten, Demokratie und Rechtsstaatlichkeit und insbesondere *mit dem Datenschutz* in Einklang zu bringen?

Die Eindämmung der Infektionen mit dem neuartigen Coronavirus, der die Lungenkrankheit Covid-19 auslöst, ist eine hinsichtlich ihrer Größenordnung und Globalität bisher unbekannte Herausforderung für demokratische Gesellschaften. Diese müssen der Pandemie und ihren Folgen entgegentreten und zugleich ihre grundlegenden Werte bewahren. Die Forderung, Datenschutz und Bürgerrechte müssten hinter der Infektionsbekämpfung zurückstehen, findet viele Befürworter, als ob Gesundheitsschutz und Datenschutz zueinander in einem Widerspruch stehen würden. Weltweit erfolgen derzeit massive Beschränkungen der Freizügigkeit, die mit Maßnahmen der Datenerfassung und Überwachung einhergehen. Diese können zur *Totalkontrolle* und zur umfassenden Zusammenführung unterschiedlichster Datenbestände führen.

Im Folgenden werden bisherige praktische Erfahrungen sowie Planungen beschrieben (Stand 01.05.2020). Dabei werden Informationen aus den Medien dargestellt, ohne dass immer durch Vergleich mit weiteren Berichten geprüft werden konnte, ob die Angaben zutreffen. Dann wird diskutiert, welche Anforderungen an einen App-Einsatz gegen die Verbreitung des Virus durch unsere freiheitliche und *demokratische Rechtsordnung* zu stellen sind, also wie bürgerrechtskonformer digitaler Gesundheitsschutz möglich ist.

2 Mit Ebolapp gegen Ebola

Die *Idee mit Smartphone-Apps* gegen die Ausbreitung von ansteckenden Krankheiten vorzugehen, hatte Michael Kölsch, Honorarkonsul der Republik Liberia in Leipzig, während der verheerenden Ebola-Epidemie in Westafrika 2014, bei der mehr als 11.000 Menschen starben. In Kooperation mit dem Verein Freunde Liberias organisierte er, dass Ärzte aus Deutschland in die Region geschickt wurden. Seine Überlegung war: „Da in Afrika fast jeder ein Mobiltelefon hat, könnte man die Technik doch vielleicht dazu verwenden, möglichst frühzeitig Menschen zu warnen, die mit Infizierten in Kontakt gekommen sind." Er glaubte, man könne die „Ebolapp", so wurde das Projekt genannt, so schnell entwickeln, dass man sie noch während des Ausbruchs in Westafrika einsetzen könnte: „Doch dann wurde mir bewusst, dass das ein Riesenprojekt ist." Es fanden sich Unterstützer, die das Projekt mit Spenden finanzierten. Programmiert hat die Software eine Leipziger Firma, auch mit viel ehrenamtlichem Einsatz. Nach fünf Jahren war die App fertig. Ein erster Testlauf an einer Leipziger Klinik war offenbar erfolgreich. Mit Hilfe von Pflegekräften und Ärzten, die die App installierten, untersuchten die Entwickler, ob die App erkennt, wenn sich andere Nutzer in der Nähe befinden.[1]

3 Von China ...

Diese Entwicklung wurde durch das *Coronavirus* (SARS-CoV-2) überholt bzw. beschleunigt. Das Virus breitet sich seit Ende 2019, von Wuhan in China ausgehend, weltweit aus. In asiatischen Ländern kamen technische Überwachungsinstrumente zum Einsatz, die zuvor zur Bekämpfung von Gesundheitsgefahren nicht denkbar waren:

In der *Volksrepublik China* war man noch nie zimperlich bei der Überwachung der Bevölkerung. Im Februar 2020 startete die dortige Regierung die Plattform „Close Contact Detector", mit der sich ermitteln lässt, wie nahe man einem Infizierten gekommen ist. Die App wertet dafür die Datenbanken öffentlicher Verkehrsmittel aus. In China müssen sich nicht nur Flug-, sondern auch Zug- und in manchen Städten sogar U-Bahnreisende mit vollem Namen und Ausweisnummer für ausgewiesene Sitzplätze registrieren. Die App gibt Auskunft darüber, ob man drei Reihen vor oder hinter einem Infizierten saß. Zudem erstellen die drei großen staatlichen Mobilfunkanbieter über ihre Kunden anhand der Funkzellenlokalisierung Bewegungsprofile für jeweils 14 Tage. Chinesische Arbeitgeber fragen diese Profile ab, bevor sie ihre Mitarbeiter aufs Firmengelände lassen.

In Hangzhou, Sitz des Onlinehändlers *Alibaba*, installierte das Unternehmen eine App namens „Gesundheitscode", bei der die Informationen der registrierten Kunden mit den Datenbanken der Gesundheitsbehörden abgeglichen werden. Über einen Farbcode wird dann die errechnete „Gefährdung" angezeigt: Grün bedeutet freie Bewegung, bei Gelb wird eine 7-, bei Rot eine 14-tägige Qua-

rantäne empfohlen. Die App teilt ihre Daten nicht nur mit den Gesundheitsbehörden, sondern auch mit der Polizei. Ende März 2020 war das Verfahren von Alibaba schon in mehr als 200 Städten der Volksrepublik eingeführt, auch in der Provinz Hubei mit der Provinzhauptstadt Wuhan, dem Ausgangsort der Pandemie. Alibaba-Konkurrent *Tencent* entwickelte und verbreitet eine ähnliche App. „Anti-Virus Code" teilt zusätzlich zum Farbcode mit, wie weit man sich gerade von einem bestätigten Coronafall aufhält. Gerät man in eine Polizeikontrolle, checkt in einem Hotel ein oder betritt einen Supermarkt, so wird man aufgefordert, die App vorzuzeigen.

Ohne *positives Rating* ist die Aufnahme von Arbeit oder die Nutzung von Bahn oder Flugzeug nicht möglich. Während einer Pressekonferenz Ende Februar wurde behördlich mitgeteilt, dass mehr als 50 Mio. Menschen in der Provinz Zhejiang den Dienst von Alibaba auf ihren Smartphones installiert hätten, ca. 90% der Bevölkerung dieser Provinz. Von den Codes seien 98,2% grün gewesen. Dies bedeutet, dass fast eine Millionen Menschen gelbe oder rote Codes zugeteilt bekommen hatten.

Täglich werden in China ca. 50.000 Tests durchgeführt. Seit Ende März durften nichtchinesische Staatsbürger nicht mehr einreisen. Chinesische Staatsbürger müssen 14 Tage vor ihrer Einreise per Flugzeug jeden Tag ihren Gesundheitsstatus über eine App melden. Bei der Einreise selbst müssen sie sich testen lassen und danach 14 Tage in eine überwachte Quarantäne begeben.[2]

Die *Weltgesundheitsorganisation* (World Health Organization – WHO) lobte den chinesischen Digitaleinsatz zur Coronabekämpfung ausdrücklich. In Sachen Informationstechnik (IT) sind viele chinesische Produkte Exportschlager, unabhängig davon, wie grundrechtskonform sie sind. Es ist naheliegend, dass das chinesische Exempel für andere Länder zum Vorbild genommen wurde.[3]

4 ... über das weitere Asien, Australien ...

In *Hongkong* wurden seit Anfang Februar Quarantänepflichtige gezwungen, mit einem Smartphone verbundene elektronische Armbänder zu tragen. Bricht die Verbindung ab oder verlässt ein Patient seine Wohnung, wird die Gesundheitsbehörde alarmiert. Die Menschenrechtlerin Maya Wang meinte, der Ausbruch des Coronavirus erweise sich als „ein Meilenstein in der Geschichte der Massenüberwachung".

In *Taiwan* wurde früh damit begonnen, „elektronische Zäune" um Menschen in Quarantäne zu ziehen. Loggt sich ein Mobiltelefon eines Infizierten in eine Funkzelle ein, die nicht seinen Wohnort abdeckt, so wird die Polizei alarmiert.

Seit 20.03.2020 wird im autoritär regierten *Singapur* mit Unterstützung des Gesundheitsministeriums durch die Singapur Government Technology Agency die freiwillige Smartphone-App „TraceTogether" verbreitet, mit der die Nutzenden über einen zentralen Server identifiziert werden. Ein hierüber vergebenes Pseudonym wird an die App gesendet, das per Bluetooth mit in der Nähe befindlichen Geräten ausgetauscht wird. Diese Daten werden an einen Zentralserver gesendet. Im Falle der Infektion werden die Kontakte ermittelt und die entsprechenden Personen informiert, um diese in Quarantäne zu schicken. In dem Stadtstaat sollen Ende April nur 20% der Menschen die App heruntergeladen haben. Die Quarantäne wird dort durch Überwachung der infizierten Personen anhand der GPS-Daten ihrer Smartphones durchgesetzt; die Infizierten müssen mithilfe von spontan abgefragten Fotos ihrer Wohnumgebung nachweisen, dass sie sich tatsächlich in ihrer Wohnung aufhalten.[4]

Die Regierung von *Südkorea* will sich nach der Masseninfektion mit MERS (Middle East Respiratory Syndrom) fünf Jahre zuvor nicht erneut dem Vorwurf aussetzen, nicht vor Infizierten gewarnt zu haben. Die Behörden versenden Textnachrichten in das Wohnviertel der Personen, die positiv getestet worden sind, mit Angaben zu Alter, Geschlecht, Nationalität und dem Bewegungsprofil der Infizierten. Die Namen der Infizierten werden nicht angezeigt, doch sind diese im Einzelfall leicht z.B. von Nachbarn herauszubekommen. In dem Land wurden millionenfach GPS-basierte Warnapps heruntergeladen. „Corona 100 Meter", „Corona Doctor" und „Corona Map" gehören zu den meistgeladenen Apps im Land.[5] Nachdem am 19.02.2020 die Zahl der Infizierten im südkoreanischen Ort Daegu rapide angestiegen war, wo kurz zuvor ein großes Sektentreffen stattgefunden hatte, wurden ausnahmslos die ca. 10.000 örtlichen Sektenmitglieder getestet. Am Ende wurden alle bekannten 240.000 Sektenanhänger im Land getestet und isoliert, ebenso wie alle Menschen, die enger mit ihnen zu tun hatten. Kontaktpersonen werden auch mithilfe von Location-Tracking von Smartphones und Kreditkartennutzungen erkannt. Dafür arbeitet die Regierung mit 3 Telekommunikations- und 22 Kreditkartenunternehmen zusammen. Bis zu 15.000 Tests werden täglich in dem Land zur frühestmöglichen Erkennung durchgeführt. Mehr als 50 südkoreanische Sonderbeamte sind hierfür abgestellt. Über die Apps werden die Menschen zudem informiert, wie hoch die Ansteckungswahrscheinlichkeit ist. Dies ermöglichte es, die weitere Ausbreitung der Infektion zu bremsen. Bis zum 16.04.2020 waren nach offiziellen Angaben in dem Land 229 Coronatote zu beklagen.[6]

Im 1,3 Milliarden-Staat *Indien* werden am Flughafen Einreisende gesundheitlich überprüft und 14 Tage in häusliche Quarantäne gesteckt. Die Adressen von Tausenden unter Quarantäne stehenden Personen werden im Bundesstaat Bangalore online veröffentlicht. Die isolierten Personen werden aufgefordert, eine App herunterzuladen, über die teilweise stündlich ein Selfie abgefordert wird. Anhand der GPS-Koordinaten in der Bilddatei kann von den Beamten der Standort festgestellt werden. Die indische Regierung hat landesweit die App Aarogya Setu („Gesundheitsbrücke") veröffentlicht, die Nutzer warnen soll, wenn sie mit Infizierten in Kontakt gekommen sind. Sie müssen ihre Handynummer, ihr Geschlecht, ihren Namen, Alter und Beruf angeben. Die App versendet regelmäßig GPS-Daten.[7]

Das in Singapur praktizierte Verfahren war Vorbild für das demokratische Australien, wo auf freiwilliger Grundlage die „COVIDSafe"-App zum Einsatz kommt. Zum Freischalten der App sind von jedem Nutzenden Name (auch Pseudonym möglich), Telefonnummer, Altersgruppe und Postleitzahl anzugeben. Die Polizei erhält keinen Zugriff auf

die Daten. GPS-Standortdaten werden nicht erfasst. Nach 21 Tagen werden die an einen zentralen Server gemeldeten Bluetooth-Kontaktdaten wieder gelöscht. Am ersten Tag der Bereitstellung hatten schon 2 Mio. Menschen die App auf ihre Geräte geladen. Die australische Gesundheitsbehörde hofft auf eine Nutzung durch gut die Hälfte der 25 Mio. Einwohnerinnen und Einwohner.[8]

5 … und Israel …

In *Israel* hat die von Benjamin Netanjahu geführte Übergangsregierung per Notstandsverordnung die Bürgerüberwachung durch Smartphonedaten in die Hände des Inlandsgeheimdienstes Schin Bet gelegt und hierbei zunächst nicht einmal das Parlament eingebunden. Im Rahmen der Coronakrise enthüllten die Journalisten Ronen Bergman und Ido Shvartztuch, dass Schin Bet eine Datenbank („das Werkzeug") besitzt, die Informationen zu jedem Bürger enthält und schon vor Corona Bewegungs- und Gesprächsdaten der Israelis sammelte. Nun löste jeder positive Coronatest eine Kette von Datenanfragen aus, über die erkundet werden sollte, mit wem die betroffene Person wo wie lange in den vergangenen zwei Wochen in Kontakt gewesen ist. Dazu wurden 14 Sensoren des Smartphones ausgewertet einschließlich GPS-Standort, Bewegung, Beschleunigung, Lichtverhältnisse, WLAN- und Bluetooth-Kontakte. Cybersecurity-Spezialist Isaac Ben-Israel erläuterte: „Man kann richtig in die Inhalte hinein, in die sozialen Netzwerke desjenigen und in seine E-Mails." Es wurde nicht offengelegt, wie die erlangten Daten mit bereits vorhandenen Daten abgeglichen werden und ob bzw. wann die Daten gelöscht werden.

Bürgerrechtsorganisationen riefen den *Obersten Gerichtshof* an, der zwar die Einberufung des Parlaments, der Knesset verlangte, aber die Überwachung vorerst bis zum 30.04. genehmigte.[9] Das Gericht forderte dann mit einer Entscheidung vom 26.04.2020 eine gesetzliche Grundlage und die Einstellung der Überwachung.

1,6 der 6,5 Mio. Smartphonebesitzer in Israel nutzen die *App „HaMagen"* (das Schutzschild), die anzeigt, ob sie sich in der Nähe eines Verdachtsfalls befinden oder befunden haben. Verteidigungsminister Naftali Bennett erwägte ein System, das die Bewegung Infizierter in Echtzeit überwacht – in Kooperation mit umstrittenen Dienstleistern für Spionagesoftware wie der Fa. NSO. Hiergegen legte das Justizministerium sein Veto ein.

6 … nach Europa

Die Berichte aus Asien führten in Europa dazu, dass auch hier digitale Coronabekämpfung auf die Tagesordnung kam.[10] In *Tschechien* wurde an der Technischen Hochschule Prag eine Anwendung „Freman contra Covid" entwickelt, die „nichts vorschreibt, nichts verbietet, niemanden verfolgt und keine persönlichen Daten sammelt". Das Programm will Menschenansammlungen verhindern, indem es Prognosen aufgrund von Bewegungsdaten trifft und z.B. dann rät, später einzukaufen.

Die auf pseudonymer Basis arbeitende App „Bleib gesund" aus der *Slowakei* warnt auf freiwilliger Grundlage Handynutzende, wenn sich ein registrierter Infizierter auf 50 Meter nähert. Zugleich kann die App überwachen, ob sich Infizierte an die Quarantäne halten. Die Regierung ließ sich mit einem „Lex Korona" das Tracken aller Mobiltelefone gestatten.

In *Polen* ist seit dem 19.03.2020 die App „Kwarantanna Domowa" (Hausquarantäne) im Einsatz, mit der die Polizei die Personen in Quarantäne digital über eine GPS-Lokalisierung kontrolliert. Davon waren Anfang April bereits 300.000 Menschen betroffen. Wer die App auf sein Gerät lädt, erhält zu wechselnden Zeiten eine SMS. Danach muss der Nutzer innerhalb von 20 Minuten ein Foto aufnehmen und abschicken. Die App ist seit dem 01.04.2020 verpflichtend. In der Praxis litt die App immer wieder an Funktionsstörungen. Die Daten sollen sechs Jahre lang gespeichert werden.[11]

Am 25.03. 2020 wurde in *Österreich* vom dortigen Roten Kreuz (ÖRK) die App „Stopp Corona" veröffentlicht. Diese tauscht eindeutige Nutzerkennungen zwischen einander nahen Smartphones aus, welche die Kontakte speichern. Im Falle einer Infektion sollen sich die Nutzer über die App beim ÖRK melden. Das verständigt über die App die Kontaktpersonen der vergangenen 3 Kalendertage. Hierbei wird u.a. auch die Mobilfunknummer der Infizierten erfasst. Entwicklung und Betrieb liegen in den Händen von Accenture; die Dienste werden in der Microsoft Azure Cloud gehostet und für die Benachrichtigungen wird Googles Firebase Cloud Messaging verwendet. Ende April 2020 war die App über 400.000 Mal installiert worden. Der Quellcode ist veröffentlicht. Die App, die Ende April noch nicht ohne Kommunikation über einen zentralen Server auskam, sollte nicht unter das gemeinsame europäische Dach von PEPP-PT gebracht werden, sondern als besonders datenschutzfreundliche Lösung zum Vorzeigemodell werden (s.u. 13).[12]

Am 08.04.2020 beschloss die EU-Kommission eine Empfehlung zur Etablierung eines Verfahrens mit den Mitgliedstaaten zur Entwicklung eines *gemeinsamen europäischen Ansatzes* („Toolbox") zum Einsatz digitaler Mittel, die es den Bürgern ermöglicht, zielgerichtet Ansteckungskontakte zu vermeiden.[13] Am 15.04.2020 veröffentlichte die EU-Kommission und der EU-Rat einen Fahrplan für die Aufhebung des Maßnahmen zur Eingrenzung von Covid-19, der u.a. die Schaffung eines Rahmens für „contact tracing and warning" mit Mobilgeräten vorsieht. Diese Maßnahme soll auf freiwilligen Einwilligungen basieren und die europäischen Datenschutznormen respektieren.[14]

Am 21.04.2020 beschloss der *Europäische Datenschutzausschuss* (EDSA, European Data Protection Board, edpd) Empfehlungen für den Einsatz von Standortdaten und Kontaktverfolgungsinstrumenten im Zusammenhang mit der Covid-19-Krankheit. Der EDSA fordert freiwillige Lösungen, lehnt die Verarbeitung von Standortdaten ab und formuliert Anforderungen zur Zweckbindung, Datensparsamkeit und Transparenz, legt sich aber nicht auf eine dezentrale oder zentrale technische Lösung fest.[15]

7 Die Diskussion in Deutschland

In Deutschland startete die offizielle Suche nach digitalen Hilfsmitteln gegen Corona Ende Februar, als ein Projektteam um Gernot Beutel von der Medizinischen Hochschule Hannover, Jens

Wille von Ubilabs und Maxim Gleser von der IPGloves ihr „Datenspende- und Aufklärungsprojekt *GeoHealth*" dem Bundesgesundheitsministerium und dem RKI präsentierte. Bisher wird mit Hilfe von Interviews der Infizierten versucht, die Wege von deren Infektion nachzuvollziehen.[16] Die Idee von GeoHealth bestand darin, auf GPS-Basis erstellte Bewegungsdaten auszuwerten und mit Farbcode das Infektionsrisiko anzuzeigen. Mit der GeoHealth-App sollten die Nutzenden „anonymisiert" ermitteln können, ob sie sich mit Infizierten über einen bestimmten Zeitraum gemeinsam an einem Ort, etwa während einer Veranstaltung oder bei einer Fahrt in öffentlichen Verkehrsmitteln aufgehalten haben. Die Infizierten sollten ihre digitalen Bewegungsprofile per „Datenspende" zur Verfügung stellen.[17]

Die *Deutsche Telekom* unterstützt das RKI seit dem 17.03.2020 mit Handydaten. Hierfür machte das Unternehmen der Behörde zunächst 5 Gigabyte seiner Kundendaten in anonymisierter Form zugänglich. Eine RKI-Sprecherin erklärte: „Damit lassen sich Bewegungsströme modellieren – bundesweit, auf Bundesland-Ebene sowie bis auf die Kreis-Gemeinde-Ebene heruntergebrochen. Ein Tracking einzelner Menschen ist damit aber nicht möglich." Von Medien und Bürgerrechtlern wurde hinterfragt, ob die gelieferten Daten wirklich aggregiert und anonym sind. Eine Telekom-Sprecherin gab bekannt, dass die Ortung in Städten auf etwa 500 Meter genau sei, auf dem Land noch ungenauer. Diese Daten werden seit 2015 zur Berechnung von Verkehrsströmen Verkehrsunternehmen oder Kommunen, also regional begrenzt, zur Verfügung gestellt. Zur Datenweitergabe an das RKI hieß es: „So umfangreiche Daten haben wir noch nie jemandem weitergegeben." Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Ulrich Kelber erklärte, die Weitergabe der Telekom-Mobilfunkdaten an das RKI sei „datenschutzrechtlich unbedenklich". Bei dem Verfahren würden mindestens 30 Datensätze zusammengefasst, um eine nachträgliche Repersonalisierung zu erschweren.[18]

Der Telekom folgten weitere Mobilfunkanbieter, die dem RKI aggregierte Mobilitätsdaten weitergaben. Der Mobilfunkanbieter A1 in Österreich stellte der dortigen Regierung ähnliche Datensätze zur Verfügung. Mitte April stellte auch Apple aus seinem Kartendienst *Apple Maps* Mobilitätsdaten öffentlich frei im CSV-Form (comma-separated values) für Analysen zum Herunterladen bereit, um Anhaltspunkte zum Erfolg von Ausgangsbeschränkungen im Kampf gegen die Ausbreitung des Virus SARS-CoV-2 zu liefern. Auf dieser Basis errechnete Apple z.B. im April, dass der Autoverkehr seit dem Lockdown in Berlin um 54% gesunken war und in München um 64%.[19]

8 Gescheiterter Gesetzgebungsversuch

In einer Formulierungshilfe für einen *Gesetzentwurf* „zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite" vom 20.03.2020 schlug das Bundesgesundheitsministerium (BMG) mit einer umfassenden Änderung des Infektionsschutzgesetzes (IfSG), die weitgehend auch später Gesetz wurde[20], im § 5 Abs. 10 IfSG vor, dass das RKI „zum Zweck der Nachverfolgung von Kontaktpersonen technische Mittel einsetzen (kann), um Kontaktpersonen von erkrankten Personen zu ermitteln". Hierfür sollte das RKI von Mobilfunkbetreibern die Standortdaten und die erforderlichen Daten der möglichen Kontaktpersonen abfragen können. Der Zweck sollte es sein, die „ermittelten Kontaktpersonen von dem Verdacht einer Erkrankung (zu) informieren". Das Bundesjustizministerium meldete verfassungsrechtliche Bedenken an, ebendies taten auch Datenschützer. Sie wiesen zudem darauf hin, dass die im Entwurf vorgesehene Funkzellenortung viel zu grob ist, um mögliche Ansteckungen zu identifizieren.[21]

9 Überall Apps

Derweil versuchen Unternehmen mit Apps und der Corona-Angst Geschäfte machen. So wurden Arbeitgeber von einem dubiosen Firmenkonsortium aufgefordert, von ihren Beschäftigten Gesundheitsdaten zu sammeln „nur € 16,90 pro Woche und Mitarbeiter". Die *„covid-19 check"*-App, sei angeblich „100% DSGVO-konform" und die Daten würden „nach ISO 27001 zertifiziert" gespeichert. Die Werbung für diesen Dienst ging unter anderem an eine Reihe von Kunden eines Unternehmens für Arbeitsschutz in Marl, wo vermutet wird, dass ein ehemaliger Mitarbeiter, der nun für den Anbieter der App Werbung betreibt, eine Kundendatei mit zahlreichen Privatadressen „mitgenommen" hatte.[22]

Die Fa. BS Software Development bewirbt eine App, mit der die *Mitteilung von Corona-Testergebnissen* beschleunigt und zugleich das Telefonnetz entlastet werden soll. Die Telekom stellt dafür eine Healthcare Cloud zur Verfügung, in der die Testergebnisse der Patienten gespeichert werden. User scannen den QR-Code eines Etiketts, das sie beim Test vom Arzt erhalten, über die App ein. Sobald das Testergebnis vorliegt, erhalten sie eine Push-Benachrichtigung, um dann das Ergebnis auf ihrem Smartphone abzurufen. Eine Überprüfung des Angebots zeigte, dass die App das Zertifikat des https-Servers nicht überprüfte, das zudem seit Jahren abgelaufen war, und dass eine veraltete Verschlüsselungstechnik zum Einsatz kam. BS Software Development musste seinen Server herunterfahren und kündigte an, eine aktualisierte Version der App zu veröffentlichen.[23]

Um unnötige Arztbesuche zu vermeiden, bei denen sich Patienten im schlimmsten Fall anstecken könnten, hat die Berliner Charité mit Unterstützung durch das Bundesgesundheitsministerium (BMG) und das RKI einen *Online-Corona-Test* veröffentlicht, über den durch die Beantwortung von 26 Fragen die Nutzenden mehr Klarheit erhalten sollen, ob eine Coronainfektion vorliegt, wozu dann weitere Handlungsempfehlungen gegeben werden.[24]

10 Die Politik

Inzwischen wurde bekannt, dass eine Basissoftware für Corona-Apps unter dem sperrigen Namen „Pan-European Privacy-Preserving Proximity Tracing", kurz PEPP-PT, in der Fertigstellung ist. Diese Entwicklung wird von der Bundesregierung sowie von den Landesregierungen unterstützt, die am 15.04.2020 Folgendes beschlossen:

Zur Unterstützung der schnellen und möglichst vollständigen Nachverfolgung

von Kontakten ist der Einsatz von digitalem „contact tracing" eine zentral wichtige Maßnahme. Bund und Länder unterstützen hierbei das Architekturkonzept des „Pan-European Privacy-Preserving Proximity Tracing", weil es einen gesamteuropäischen Ansatz verfolgt, die Einhaltung der europäischen und deutschen Datenschutzregeln vorsieht und lediglich epidemiologisch relevante Kontakte der letzten drei Wochen anonymisiert auf dem Handy des Benutzers ohne die Erfassung des Bewegungsprofils speichert. Darüber hinaus soll der Einsatz der App auf Freiwilligkeit basieren. Sobald auf Grundlage der bereits vorgestellten Basissoftware eine breit einsetzbare Anwendungssoftware (App) vorliegt, wird es darauf ankommen, dass breite Teile der Bevölkerung diese Möglichkeit nutzen, um zügig zu erfahren, dass sie Kontakt zu einer infizierten Person hatten, damit sie schnell darauf reagieren können. Bund und Länder werden dazu aufrufen. Ferner werden alle diejenigen, die unabhängig davon an Tracing-Apps arbeiten, eindringlich gebeten, das zugrundeliegende Architekturkonzept zu nutzen, damit alle Angebote kompatibel sind. Ein Flickenteppich von nicht zusammenwirkenden Systemen würde den Erfolg der Maßnahme zunichte machen.

Nach Auseinandersetzungen mit der Architektur von PEPP-PT zogen sich aus dem Projekt viele Partner, auch aus Deutschland zurück (s.u. 13). In dieser ohnehin schwierigen Situation brachte Bundesgesundheitsminister Jens Spahn am 20.04.2020 auf einer Pressekonferenz, bei der es insbesondere um eine bessere Ausstattung der Gesundheitsämter ging, eine *„Quarantäne-App"* ins Gespräch, mit der die Einhaltung der Quarantäne überwacht werden könne. Auf Presseanfragen hin verwies das BMG auf einen Beschluss des Corona-Kabinetts, in dem von einem „Quarantäne-Tagebuch" die Rede ist. Mit diesem wolle man das Personal in den Gesundheitsämtern bei der „Überwachung der in häuslicher Quarantäne befindlichen Bürgerinnen und Bürger" entlasten. Die Kontrolle des aktuellen gesundheitlichen Zustandes erfolge aktuell durch zwei Anrufe oder Hausbesuche pro Tag. Zur Vereinfachung des Prozesses werde das BMG den Gesundheitsämtern eine Plattform zur Verfügung stellen, die eine digitale Abfrage der Symptome ermögliche – die Anwendung solle für Nutzer freiwillig sein, für die Ämter hingegen verpflichtend. Die für Digitalpolitik zuständigen Jens Zimmermann (SPD-Bundestagsfraktion) und Maria Klein-Schmeink (Grüne) äußerten umgehend die Befürchtung, die neue App solle auch zur „Kontrolle der Quarantäne-Maßnahmen" genutzt werden, wodurch zugleich der Erfolg der Warn-App aufs Spiel gesetzt werde.[25]

11 PEPP-PT

Hinter PEPP-PT steht die EU-Kommission, die versucht, sich unter den EU-Mitgliedern auf gemeinsame Standards zu verständigen (s.o. 6). Dadurch soll es auch möglich sein, grenzüberschreitend Corona-Warnungen zu kommunizieren. Zu Beginn entwickelten 130 europäische Wissenschaftler und IT-Experten, koordiniert von Chris Boos, IT-Unternehmer der Fa. Aarago, eine Basissoftware für Corona-Apps. Die Plattform ist ein Software-Gerüst, auf dem App-Entwickler aufsetzen können. Der Quellcode sollte unter der Open-Source-Lizenz der Mozilla Foundation veröffentlicht werden. An der deutschen Entwicklung beteiligten sich das RKI und das Heinrich-Hertz-Institut. Maßgeblich beteiligt war auch die Ecole Polytechnique Fédérale de Lausanne (EPFL). Das Konzept basiert auf Bluetooth-Low-Energy-Funktechnik (BLE). Die Nutzung soll besonders energiesparend sein und nur einige Meter weit reichen. Jedes Handy, das die Software lädt, erhält eine zufällige Identifikations-(ID-)Nummer, die sich alle 30 Minuten ändert. Andere Geräte, die sich für einen bestimmten Zeitpunkt in der kritischen Reichweite von weniger als zwei Meter befinden, werden mit ihrem Pseudonym lokal verschlüsselt gespeichert. Nach einer positiven Diagnose überträgt der Erkrankte die Liste der IDs auf einen zentralen Server. Dieser fordert per Push-Nachricht die Kontaktpersonen auf, sich testen zu lassen. Persönliche Informationen, Standortdaten oder andere Merkmale würden nicht gespeichert. Ältere Daten, die keinen epidemiologischen Wert mehr haben, werden automatisch gelöscht.[26]

Bei der Entwicklung in Deutschland wurden der Bundesdatenschutzbeauftragte (BfDI) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingebunden. Es bestand Konsens unter allen Beteiligten, dass es keine App-Nutzungspflicht geben soll. Die Wissenschaftler hoffen, dass 60% der Bevölkerung eine solche App nutzen. Dies wären bundesweit 50 Mio. Menschen. Da vor allem ältere, besonders gefährdete Menschen oft kein Smartphone nutzen, sollten Bluetooth-Armbänder oder andere tragbare Geräte verteilt werden. In einer Umfrage der Universität Oxford haben etwa 70% der Deutschen signalisiert, dass sie sich eine Nutzung einer solchen Tracing-App vorstellen können.

Das PEPP-PT-Projekt mit seinem technischen Gerüst und dem vorgesehenen Zertifizierungsrahmen war zwar kein offizielles EU-Vorhaben. Doch will die *EU-Kommission* für eine einheitliche Referenzimplementierung eine Art politischen und rechtlichen Überbau schaffen. Zugleich will sie Apps verhindern, die gegen das europäische Datenschutzrecht verstoßen. Über die Zusammenarbeit mit dem Europäischen Zentrum für Prävention und die Kontrolle von Krankheiten (ECDC) soll zudem ein Datenaustausch mit öffentlichen Stellen in aggregierter Form sichergestellt werden.[27] Am 15.04.2020 veröffentlichte das eHealthNetwork, das Netzwerk für elektronische Gesundheitsdienste der EU-Mitgliedstaaten, ein 44-seitiges Papier, das die Anforderungen für Bluetooth-basierte Tracing-Dienste klarstellt und präzisiert: Freiwilligkeit, staatliche Anerkennung, Datenschutzkonformität und zeitliche Begrenzung.[28] Das Konzept baut auf Empfehlungen des Europäischen Datenschutzausschusses (EDSA/epdb) von 14.04.2020 auf, die darlegen, dass für Zwecke der Kontaktverfolgung und Warnung eine Lokalisierung unnötig ist, und dass lokale Verarbeitungslösungen zentralisierten Verfahren vorzuziehen sind.[29]

Es sollte *mehrere Apps* auf einer gemeinsamen technischen Grundlage in Deutschland geben, u.a. eine vom RKI. Die Initiative „gemeinsam gesund" ist von Anfang an eingebunden. Zwecks Koordinierung bedarf es einer zentralen Stelle. Die Apps müssen sich von dem Entwickler-Konsortium zertifizieren lassen. Die Corona-Warn-Apps auf

Basis der PEPP-PT-Plattform sollten je nach Land verschiedene zusätzliche Funktionalitäten enthalten können, etwa zur Kommunikation mit den Gesundheitsämtern. Boos erklärte: „Wie das ausgestaltet werden wird, wird jedes Land entsprechend seiner gesetzlichen Regelungen für sich entscheiden." Entscheidend sei, dass ohne die freiwillige Einwilligung der Nutzer keinerlei Daten übertragen werden. Er wies jedoch auch darauf hin, dass es sich in Deutschland bei Covid-19 um eine meldepflichtige Erkrankung handelt. Die Betroffenen sind also verpflichtet, sich persönlich bei ihrem Gesundheitsamt zu melden. „Dies kann möglicherweise über eine App abgebildet werden."[30]

12 Zwei US-Unternehmen

Die Hersteller der mobilen Betriebssysteme *Apple (iOS) und Google (Android)* kündigten am 10.04.2020 gemeinsam an, sie wollten Bluetooth-Funktechnik nutzen, um Kontaktpersonen von Corona-Infizierten frühzeitig zu ermitteln, ohne die Identität der Beteiligten zu offenbaren. Ähnlich wie beim PEPP-PT-Konzept verschicken Smartphones über die Bluetooth-Technik BLE ständig eine Identifikationsnummer (ID), die dann andere Handys in der Nähe speichern. So soll im Nachhinein festgestellt werden, welche Geräte – und damit in den meisten Fällen auch deren Besitzer – sich lange genug räumlich nahe genug waren, um eine Ansteckung zu befürchten. Wer später positiv auf das Virus getestet wird, kann seine ID im System veröffentlichen. Die Geräte derjenigen Nutzer, die in der Nähe dieser ID waren, werden benachrichtigt und z.B. aufgefordert, sich testen zu lassen. Die Geräte-IDs, die täglich gewechselt werden, sollen nie einer bestimmten Person zugeordnet werden. Eine Erfassung von Standortdaten soll nicht erfolgen.[31] Die Schnittstellen in iOS und Android sollten umgehend geöffnet werden, damit Gesundheitsbehörden diese weltweit in ihre eigenen Apps einbauen können. Über die Schnittstellen, auf die ausschließlich von hoheitlich autorisierten Apps zugegriffen werden können soll, kommunizieren auch die jeweiligen Apps der iOS- und der Android-Geräte untereinander. Covid-19-Diagnosen müssen demnach von Ärzten oder Laboren bestätigt werden, um das Risiko von Fehlalarmen zu reduzieren und Trolle abzuschrecken, die das System mit absichtlichen Fehlalarmen stören könnten.

In einem zweiten Schritt wollen Apple und Google die Bluetooth-Tracing-Funktion direkt in ihre jeweiligen *Betriebssysteme integrieren*. Nutzer müssten dann keine App mehr herunterladen, sondern nur noch der Nutzung zustimmen. Hat das System einen Risikokontakt bestätigt, sollen Nutzer jedoch auch aufgefordert werden, zusätzlich eine entsprechende App der jeweiligen Gesundheitsbehörden ihres Landes zu installieren. Nur diese zertifizierten Apps sollen laut Apple und Google Zugriff auf die Daten bekommen.

Das Massachusetts Institute of Technology in Cambridge/USA (MIT) arbeitet an einem ähnlichen System unter dem Namen „Safe Paths".[32] Der Kryptografie-Experte Moxie Marlinspike, Entwickler des Verschlüsselungs-Protokolls im Messenger Signal, wies aber auf die Gefahr hin, dass über die bestehende Bluetooth-Tracking-Infrastruktur die Werbeindustrie die IDs sammeln und so in Erfahrung bringen könne, wer Covid-positiv ist.[33]

13 Kritik an PEPP-PT

Am 20.04.2020 warnten 300 internationale Wissenschaftler in einem *Brandbrief* an die Politik davor, dass einige der Lösungen für Kontaktverfolgung-Apps, „schleichend zu Systemen führen könnten, die eine noch nie dagewesene Überwachung der Gesellschaft als Ganzes ermöglichen würden". Systeme, die eine Rekonstruktion des „sozialen Graphen" einer Person erlauben, sollten „ohne weitere Diskussion" abgelehnt werden. Sie weisen darauf hin, dass Google und Apple von Befürwortern zentral organisierter Lösungen unter Druck gesetzt werden, ihre Systeme für umfangreichere Datenerfassungen zu öffnen. Zu den Unterzeichnern der Stellungnahmen gehören zahlreiche Mitglieder wissenschaftlicher Akademien, Fellows von prominenten IT-Verbänden wie Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE) und International Association for Cryptologic Research (IACR) sowie viele deutsche Wissenschaftler, die im Bereich Computersicherheit oder in angrenzenden Themengebieten arbeiten.

Die Wissenschaftler formulierten vier allgemeine *Anforderungen* an ein vertrauenswürdiges Contact-Tracing-System: So dürften die Kontaktverfolgungs-Apps ausschließlich eingesetzt werden, um Covid-19 einzudämmen. Das System dürfe nicht in der Lage sein, mehr Daten zu sammeln, als zu diesem Zweck notwendig ist. Jedes in Betracht kommende System müsse „vollkommen transparent" sein, einschließlich der Protokolle und ihrer Implementierungen sowie der Teilkomponenten. Es müsse immer die technische Option gewählt werden, die die Privatsphäre besser schütze. Schließlich müsse die Nutzung der Apps freiwillig sein. Die Systeme sollten nach der aktuellen Krise abgeschaltet werden und die Daten müssten alle gelöscht werden können.

Schon in den Tagen zuvor hatten sich zahlreiche Projektpartner, insbesondere aus den Bereichen IT-Sicherheit, Datenschutz und Privatsphäre, von PEPP-PT distanziert. Die Kontakte zu den Wissenschaftlern, die an einer dezentralen Architektur unter dem Namen „DP3T (Decentralized Privacy-Preserving Proximity Tracing)" gearbeitet hatten, waren auf Arbeitsebene abgebrochen worden. Ninja Marnau vom CISPA Helmholtz Center for Information Security, begründete den CISPA-Rückzug damit, dass es sich bei dem Konzept „um einen zentralen Ansatz mit unrealistischen und risikoreichen Vertrauensannahmen handelt. Außerdem ist nicht klar, ob tatsächlich der gesamte Code veröffentlicht werden wird." Es sei problematisch, dass es sich bei PEPP-PT nicht um eine Plattform mit verschiedenen Ausprägungen, sondern lediglich um eine Kommunikationsplattform von verschiedenen Projekten handeln soll. Mehrere Länder würden sehr unterschiedliche Ansätze verfolgen, die nicht miteinander interoperabel seien. Auch die Turiner Forschungsstiftung ISI (Istituto per l'Interscambio Scientifico), die Eidgenössischen Technischen Hochschulen (ETH) Zürich und Lausanne sowie die Katholische Universität Leuven zogen sich vom PEPP-PT zurück und ori-

entierten sich nur noch auf das dezentrale Projekt DP3T.[34]

14 Datenspeicherung und -abgleich dezentral

Am 26.04.2020 erfolgte dann eine erstaunliche Wende der deutschen Bundesregierung in der Warn-App-Diskussion. Bisher hatte sie auf PEPP-PT mit einer serverbasierten Abgleichs- und Kommunikationslösung gesetzt. Nach massiver öffentlich geäußerter Kritik an PEPP-PT drohte die Akzeptanz für die Lösung zu schwinden. Zuletzt hatten der Chaos Computer Club e.V (CCC), D64, LOAD e.V., das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF), die Gesellschaft für Informatik (GI) und die Stiftung Datenschutz in einem offenen Brief an Bundesgesundheitsminister Jens Spahn und Kanzleramtschef Helge Braun gewarnt, die geplante zentrale Lösung sei „höchst problematisch".[35] Ungewollt gefördert haben den Schwenk möglicherweise die für den Gesundheitsschutz zuständigen Kommunen, die als Deutscher Landkreistag in einem Brief an Spahn und Braun forderten, alle mit der Tracing-App gesammelten Daten auswerten zu können. Fraglich war schließlich, inwieweit die PEPP-PT-Lösung mit den durch Apple und Google bereit gestellten Schnittstellen technisch umsetzbar gewesen wäre. Die Regierung favorisiert nun ein *dezentrales Modell*. Dabei übermitteln die Smartphones nur ihre Schlüssel (IDs) auf einen Server. Andere Geräte fragen diese Liste regelmäßig ab, ob eine der IDs in ihrem Kontakttagebuch auftaucht.

Das nun zu verwirklichende Modell orientiert sich am DP3T-Konzept. Mit der Entwicklung wurden neben CISPA in Deutschland auch die Deutsche Telekom und SAP beauftragt. Für die Auswahl der Unternehmen soll eine Rolle gespielt haben, dass diese beiden deutschen Firmen „auf Augenhöhe" mit Google und Apple verhandeln könnten. Die Veröffentlichung sollte, so Spahn in den „nächsten Wochen" erfolgen. Die Schweiz kündigte an, den dezentralen Ansatz bereits zum 11.05.2020 im Land einzuführen. Integriert werden soll in die deutsche Tracing-App auch die Möglichkeit, dass Bürger freiwillig, in pseudonymisierter Form, Daten zur epidemiologischen Forschung und Qualitätssicherung an das Robert-Koch-Institut übermitteln können. Dazu sollen unter anderem bereits von der Fraunhofer-Gesellschaft entwickelte Komponenten genutzt werden.[36]

15 Gesundheit gegen Bürgerrechte?

Während zu Beginn der Coronakrise die vom Staat geforderten einschränkenden Maßnahmen von der großen Mehrheit akzeptiert wurden, tauchen seit März 2020 *zunehmend kritische Stimmen* auf, die forderten, den „Lockdown" zurückzufahren. Zwei Begründungsmuster dominieren dabei: Zum einen wird der ökonomische Stillstand beklagt. Die Wirtschaft müsse wieder hochgefahren werden, um zu vermeiden, dass die Nebenwirkungen der Coronabekämpfung schlimmere Effekte verursachen als das Virus selbst. Zum anderen wird rechtsstaatlich argumentiert: Staatsrechtler klagten, wir lebten in einem „Krankheitsabsolutismus" (Uwe Volkmann, Universität Frankfurt), in einem „quasi grundrechtsfreien Zustand" (Christoph Möllers, Humboldt-Universität Berlin); wir stünden „vor Hygienemaßnahmen ganz anderer Art: Der Rechtsstaat ist schwer beschmutzt. Die rechtsstaatliche Hygiene muss dringend wieder hergestellt werden, sonst droht hier das größte Infektionsrisiko" (Oliver Lepsius, Universität Münster).[37] Edward Snowden, der 2013 das weltumspannende Überwachungssystem der britischen und US-amerikanischen Geheimdienste offengelegt hat, sprach von einer „Architektur der Unterdrückung", die, wenn auch in bester Absicht, in Reaktion auf Corona entsteht.[38]

Die Warnungen vor einem Abbau freiheitlicher und rechtsstaatlicher Garantien sind nicht unbegründet. Doch ist die Situation nicht einzigartig: Bei jedem politischen und gesellschaftlichen Umbruch gibt es Kräfte, die diesen zu nutzen versuchen, um *autoritäre Strukturen zu stärken*. Die deutsche Gesellschaft hat Erfahrung mit solchen Bestrebungen, die nun Corona zu nutzen versuchen. Es geht nun darum, die Grundlagen unserer Gesellschaft zu wahren, zu denen sowohl der Gesundheitsschutz als auch die Wahrung unserer bürgerlichen Freiheiten gehören. Die Aufgabe besteht darin, angesichts einer neuen Herausforderung die Verhältnismäßigkeit staatlicher Eingriffe sicherzustellen, also dafür zu sorgen, dass die ergriffenen Maßnahmen mit ihren Grundrechtseinschränkungen geeignet, erforderlich und angemessen sind, um ein grundrechtswahrendes Ziel zu erreichen.

16 Unsichere Fakten und Bewertungsgrundlagen

Das Problem beim Coronavirus ist, dass dieses vor wenigen Monaten noch völlig *unbekannt und unerforscht* war. Ausbreitungswege, Risiken und Bekämpfungsmöglichkeiten waren und sind weiterhin in vieler Hinsicht unklar. Dies bedingt, dass die Politik zu einem Vorgehen gezwungen ist, das von Versuch und Irrtum geprägt ist. Das Problem der Unsicherheit wird dadurch verstärkt, dass etwa die Hälfte der Coronainfektionen offenbar präsymptomatisch erfolgt, also bevor der Überträger des Virus überhaupt Anzeichen einer Krankheit bemerkt hat. Effekte von Maßnahmen lassen sich nur mit Zeitverzögerung messen.

Grundlage für alle Maßnahmen muss in einem aufgeklärten Rechtsstaat sein, dass sämtliche Maßnahmen trotz der Unkenntnis vieler Wirkmechanismen – soweit wie möglich – *wissenschaftlich begründet* sind.

Es gibt keine klaren Vorgaben, wie die *Grundrechte in Beziehung* zueinander zu stellen sind. Nach unserem Verfassungsverständnis gibt es keinen Vorrang eines Grundrechtes, weder der unternehmerischen Freiheit (Art. 16 GRCh), die z.B. in seiner US-amerikanischen Lesart der US-Präsident Donald Trump über alles stellt, oder auch nicht des Grundrechts auf körperliche Unversehrtheit und auf Gesundheit (Art. 2 Abs. 1 GG, Art. 3, 35 GRCh).[39]

17 Abwägen

Auch in der Coronakrise ist der Schutz der Persönlichkeitsrechte eine „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens".[40] Kommen Apps zum Einsatz, ist nicht nur das Grundrecht auf Datenschutz,

sondern sind möglicherweise auch das Telekommunikationsgeheimnis (Art. 10 GG, Art. 7 GRCh), der Schutz der Familie (Art. 6 GG, Art. 7 GRCh), das Wohnungsgrundrecht (Art. 13 GG, Art. 7 GRCh) und die Freizügigkeit (Art. 11 GG, Art. 21 AEUV) betroffen. Auch dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG) und den diesen konkretisierenden Grundrechten kommt kein grundsätzlicher Vorrang zu. Nötig ist eine *praktische Konkordanz der Grundrechte*.

Maßnahmen dürfen nicht vorschnell ergriffen werden. Sie bedürfen der sorgsam abwägenden Bewertung und einer gesetzlichen Eingriffsgrundlage. Sie dürfen nicht dauerhaft erfolgen und müssen auf ihre Berechtigung hin immer wieder überprüft werden. Alle neu erwogenen Maßnahmen müssen sich daran messen lassen, ob sie für eine wirkungsvolle Pandemiebekämpfung wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der *Verhältnismäßigkeit* einhalten. Notfallmaßnahmen dürfen nicht zu einer langwirkenden Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger führen. Die Menschen erwarten von allen Beteiligten, dass sie die für die Vorsorge und Bekämpfung der Pandemie notwendigen Informationen zur Verfügung stellen und die Maßnahmen nachvollziehbar und transparent begründen.

Damit einher geht die Pflicht der Verantwortlichen zum sorgsamen Umgang mit personenbezogenen Daten. Das Recht des Einzelnen auf Schutz seiner personenbezogenen Daten – insbesondere soweit es sich um Gesundheitsdaten handelt – steht auch in Krisenzeiten nicht zur Disposition der Gesetzgeber oder der Behörden. Bei der Auslegung des Datenschutzrechts müssen die lebens- oder gesundheitswichtigen Interessen der Menschen und der Gesellschaft berücksichtigt werden. Das Recht verlangt auch insofern von den Verantwortlichen eine *sachgerechte Interessenabwägung*.[41]

18 Rechtsgrundlagen

Die Rechtslage zur Pandemiebekämpfung ist übersichtlich: Es gilt das allgemeine *Polizeirecht*, wonach die Polizei und die Ordnungsbehörden die Befugnis haben, die zur Abwehr einer konkreten Gefahr notwendigen Maßnahmen zu ergreifen. Neben der polizeirechtlichen Generalklausel, die aber nur die Abwehr einer konkretisierten Gefahr gegen eine bestimmte Person per Verwaltungsakt ermöglicht, gibt es das Instrument der Allgemeinverfügung, das Gefahren abwehrende Maßnahmen gegenüber einem größeren Adressatenkreis vorsehen kann. Ob dem Staat ein Nothilferecht zusteht, ist stark umstritten; dieses beschränkt sich aber in jedem Fall auf die Abwehr von im Hinblick auf Ort, Zeit und Personen konkretisierten Gefahren.

Das Katastrophenschutzrecht der Länder sieht bisher keine spezifischen informationellen Maßnahmen vor. Anwendbar ist das *Infektionsschutzgesetz* des Bundes (IfSG).

Die Nationale Akademie der Wissenschaften *Leopoldina* schlug in ihrer 3. Ad-hoc-Stellungnahme vom 13.04.2020 vor, den Rechtsrahmen des Datenschutzes im Zusammenhang mit der Pandemiebekämpfung zu überprüfen: „Angesichts der Erfahrung der derzeitigen Pandemie sollten auf europäischer Ebene die Datenschutzregelungen für Ausnahmesituationen überprüft und ggfs. mittelfristig angepasst werden. Dabei sollte die Nutzung von freiwillig bereit gestellten personalisierten Daten, wie beispielsweise Bewegungsprofilen (GPS-Daten) in Kombination mit Contact-Tracing in der gegenwärtigen Krisensituation ermöglicht werden.“[42] Diese Passage der Stellungnahme spielte in der weiteren Diskussion um notwendige Maßnahmen zwar keine wesentliche Rolle, lässt aber erkennen, dass von den Wissenschaftlern der aktuell geregelte Datenschutz als ein Hindernis zur Covid-19-Bekämpfung angesehen wird.

19 Infektionsschutzgesetz

Die Anwendung des IfSG als spezielles Gefahrenabwehrrecht führt dazu, dass in den geregelten Bereichen der Rückgriff auf das allgemeine Polizeirecht ausgeschlossen ist. In § 4 Abs. 1 IfSG ist dem Robert Koch-Institut (RKI) als zuständiger nationaler Behörde die Befugnis eingeräumt, im Rahmen von Maßnahmen zur Überwachung, Verhütung und Bekämpfung von übertragbaren Krankheiten, soweit erforderlich, personenbezogene Daten zu verarbeiten. Nach § 4 Abs. 3 IfSG ist das RKI auch zur internationalen Kooperation befugt zur Vorbeugung einer möglichen grenzüberschreitenden Ausbreitung übertragbarer Krankheiten und zur dauerhaften wissenschaftlichen Zusammenarbeit. Es darf auch insofern im Rahmen der Erforderlichkeit personenbezogene Daten austauschen.

Angesichts der neuen Herausforderungen durch die Corona-Pandemie wurde das Gesetz im März 2020 ergänzt insbesondere um die §§ 5, 5a mit Regelungen zur „Epidemischen Lage von nationaler Tragweite“.[43] In § 5 Abs. 2 Nr. 1, 2 IfSG ist vorgesehen, dass „ausschließlich zur Feststellung und Verhinderung einer Einschleppung einer bedrohlichen übertragbaren Krankheit“ von Einreisenden und Beförderungsunternehmen personenbezogene Daten erhoben werden dürfen. In den §§ 6 ff. IfSG ist ausführlich und detailliert die *Meldepflicht* von Verdächten, Erkrankungen und Todesfällen zu spezifischen Krankheiten normiert einschließlich innerdeutscher (§ 11 IfSG) und völker- und unionsrechtlicher (§ 12 IfSG) Übermittlungen. Die Meldepflicht des Coronavirus (2019-nCoV) wurde mit der Verordnung über die Ausdehnung der Meldepflicht nach §§ 6 Abs. 6 S. 1 Nr. 1, 7 Abs. 1 S. 1 IfSG des BMG vom 30.01.2020 (CoronaVMeldeV) eingeführt. Im Rahmen der Meldepflicht sind neben Namen, weiteren Identifizierungsdaten sowie präzisen Angaben zur Krankheit anzugeben, die „k) wahrscheinliche Infektionsquelle, einschließlich der zugrunde liegenden Tatsachen, l) in Deutschland: Landkreis oder kreisfreie Stadt, in dem oder in der die Infektion wahrscheinlich erworben worden ist, ansonsten Staat, in dem die Infektion wahrscheinlich erworben worden ist“ (§ 9 Abs. 1 Nr. 1 IfSG). Gemäß § 14 IfSG richtet das RKI ein elektronisches Melde- und Informationssystem ein.

§ 16 Abs. 1 S. 1 IfSG erlaubt den zuständigen Behörden, also dem RKI, den obersten Landesgesundheitsbehörden sowie den nachgeordneten Gesundheitsämtern der Städte und Kreise (§ 54 IfSG), nach Feststellung von Tatsachen, „die zum Auftreten einer übertragbaren

Krankheit führen können“, die „notwendigen Maßnahmen zur Abwendung der dem Einzelnen oder der Allgemeinheit hierdurch drohenden Gefahren“ zu treffen. In Satz 2 wird dann festgestellt: „Die bei diesen Maßnahmen erhobenen personenbezogenen Daten dürfen *nur für Zwecke dieses Gesetzes* verarbeitet werden.“

Die *konkrete Bekämpfung* übertragbarer Krankheiten wird in den §§ 24 ff. IfSG geregelt. Dabei besteht für die Feststellung und Heilbehandlung der meldepflichtigen Krankheiten ein Arztvorbehalt (§ 24 S. 1). Die Gesundheitsämter dürfen die „erforderlichen Ermittlungen“ durchführen (§ 25 Abs. 1). § 28 Abs. 1 IfSG erlaubt „die notwendigen Schutzmaßnahmen“ gegenüber Kranken, Krankheits- und Ansteckungsverdächtigen sowie Ausscheidern, insbesondere deren Beobachtung (§ 29 IfSG), die Quarantäne (§ 30 IfSG) und ein berufliches Tätigkeitsverbot (§ 31 IfSG).

Auch nach der aktuellen Änderung des IfSG setzen alle informationellen Maßnahmen zumindest einen *Ansteckungsverdacht* sowie die konkrete Erforderlichkeit der Erfassung und Verarbeitung von Daten voraus. Dies bedeutet, dass informationelle Maßnahmen gegenüber Personen im Vorfeld einer möglichen Ansteckung weiterhin unzulässig sind. Die Erfassung von Menschen ohne einen konkreten Verdacht ist unzulässig, wenn nicht die Betroffenen hierzu ausdrücklich ihre Einwilligung erteilt haben (Art. 9 Abs. 2 lit. a DSGVO). Bei einer Einwilligung ist Voraussetzung, dass diese sich im Rahmen der gesetzlichen Aufgabe der Behörde bewegt, diese freiwillig erteilt wird und zuvor eine umfassende Aufklärung erfolgte. Zur Freiwilligkeit gehört auch die jederzeitige Widerrufbarkeit, was die weitere Verarbeitung der erlangten Daten verhindert (Art. 7 Abs. 3 DSGVO).

20 Zwecke von Apps

Bei der Diskussion, was aus Datenschutzsicht zur Coronaeindämmung nötig und erlaubt ist, kommt es darauf an, welche *Zwecke* mit den einzusetzenden Instrumenten verfolgt werden. Dabei stehen im EU-Kontext das Verfolgen von Infektionswegen und die frühzeitige Warnung möglicher Infizierter im Vordergrund. Außerdem geht es dem RKI um die Nutzung erlangter Daten für Forschungszwecke unter dem Stichwort „Datenspende“, wobei hierbei der Datenschutz leider zumeist nur am Rande adressiert wird. Apps können zur einfachen und schnellen Kommunikation zwischen Betroffenen und Behörden genutzt werden. Ein Blick in andere Staaten, insbesondere in Asien, aber auch z.B. nach Polen, zeigt, dass Daten für repressive Zwecke genutzt werden, etwa zur Kontrolle von Quarantänemaßnahmen und zu deren sanktionierender Durchsetzung.[44] Bisher scheint in der EU aber weitgehend Konsens zu bestehen, dass solche repressiven Maßnahmen weder zielführend, geschweige denn – mangels gesetzlicher Grundlage und Verhältnismäßigkeit – zulässig sind.

Skepsis ist aber auch bei den präventiven Maßnahmen berechtigt, die regelmäßig damit beworben werden, dass sie freiwillig und anonym seien. Von *Anonymität* kann bei den Tracing-Apps keine Rede sein, da deren Zweck es ist, individualisierte Rückmeldungen zu geben. Korrekterweise handelt es sich dabei um pseudonyme, also personenbeziehbare Datenverarbeitung.[45] Von der Qualität des Pseudonymisierungsverfahrens hängt es ab, wie groß das Risiko einer zweckwidrigen Reidentifizierung ist.

Freiwilligkeit ist bei der Seuchenbekämpfung nicht unabdingbar. Sie ist aber in einer freiheitlichen Gesellschaftsordnung wie der unseren von zentraler Bedeutung dafür, dass viele Menschen sich nachhaltig und engagiert beteiligen.[46] Lässt sich ein Ziel nicht ohne staatlichen Zwang realisieren, dann bedürfte es einer *gesetzlichen Regelung*, die ein überwiegendes öffentliches Interesse im Bereich der öffentlichen Gesundheit verfolgt (Art. 9 Abs. 2 lit. i DSGVO).

21 Einwilligung

In Deutschland und in der EU besteht derzeit weitgehend Konsens, dass jede App-Anwendung auf einer *Einwilligung* basieren muss. Bei Angaben zu Infektionen handelt es sich um Gesundheitsdaten, ebenso, wenn z.B. Daten zu Körpertemperatur, Puls, Blutdruck usw. über Wearables erhoben werden. Dies gilt auch für weitere Angaben, etwa soziale Kontakte, Aufenthaltsorte und -zeiten, wenn diese mit den medizinischen Angaben kombiniert sind. Es kommt dann Art. 9 Abs. 1, 2 lit. a DSGVO zur Anwendung, wonach die Einwilligung sich ausdrücklich auf diese Datenverarbeitung beziehen muss. Bei der digitalen Überwachung sozialer Kontakte, auch wenn sie auf Einwilligungen basiert, ist höchste Vorsicht geboten. Sie eignet sich als Einfallstor für weitere Begierden, wie etwa die verpflichtende Nutzung solcher Apps.[47] Lokalisierungsdaten haben ebenso eine hohe Sensitivität, da über sie Bewegungsbilder erstellt und viele Rückschlüsse auf weitere Umstände möglich sind.

Voraussetzung für eine wirksame Einwilligung ist die Freiwilligkeit, Bestimmtheit und Eindeutigkeit der Willensbekundung zur Verarbeitung (Art. 4 Nr. 11 DSGVO). Die Einwilligung muss jederzeit mit Wirkung für die Zukunft widerrufbar sein (Art. 7 Abs. 3 DSGVO). Mitunter wird die *Freiwilligkeit* wegen des sozialen Drucks zur Nutzung von Apps in Frage gestellt.[48] Geht dieser Druck von staatlicher Seite aus, etwa wenn von einer App-Nutzung bestimmte Leistungen der Daseinsvorsorge abhängig gemacht werden, fehlt es an der Freiwilligkeit. Dies ist der Fall, wenn die Nutzung einer App zur Bedingung gemacht wird für die individuelle Lockerung von Ausgangsbeschränkungen oder für den Zugang zu öffentlichen oder privaten Gebäuden oder zum öffentlichen Personenverkehr. An der Freiwilligkeit bestehen aber auch Zweifel, wenn Private, etwa Gaststätten oder Versicherungen die App-Nutzung zur Voraussetzung für Leistungen machen (Art. 7 Abs. 4 DSGVO). Apps müssen nach Belieben installiert oder deinstalliert werden können.[49] Keine relevante Beeinträchtigung der Freiwilligkeit entsteht dadurch, dass, wie bei der Tracing-App, von politisch Verantwortlichen darauf hingewiesen wird, dass deren Wirksamkeit von einem hohen Nutzungsgrad abhängt, und wenn für deren Verwendung geworben wird.

22 Datenschutzgrundsätze

Transparenz für die Betroffenen ist ein grundsätzliches Erfordernis jeder Datenverarbeitung (Art. 5 Abs. 1 lit. a DSGVO) wie auch zentrale Bedingung

für die Informiertheit der Einwilligung. (Art. 4 Nr. 11 DSGVO). Die Art. 12 ff. DSGVO machen hierzu Vorgaben. Das Transparenzerfordernis bezieht sich auf die konkrete Datenverarbeitung, die verfolgten Zwecke und die ergriffenen Schutzmaßnahmen. Die Erforderlichkeit einer Maßnahme muss plausibel begründet werden. Ist dies, wie im konkreten Zusammenhang oft, nur beschränkt möglich, so muss dies offen kommuniziert werden.

Zur Transparenz gehört es, dass die eingesetzte Software *unabhängig überprüft* wird und werden kann. Ein mögliches Instrument hierfür kann die Zertifizierung nach Art. 42 DSGVO sein. Eine aus Datenschutzsicht eher fragwürdige Zulassung von digitalen Gesundheits-Anwendungen sieht der Ende 2019 eingeführte § 33a SGB V vor. Valide ist dagegen eine Veröffentlichung des Programmcodes als Open Source, so dass dieser kritisch von Experten hinterfragt und bewertet werden kann.[50]

Ein zentraler Grundsatz des Datenschutzes ist die *Richtigkeit* der Daten. Die Relevanz des Grundsatzes nimmt zu, je wichtiger der damit verfolgte Zweck ist. So muss die Richtigkeit von Wearabledaten gewährleistet sein, wenn diese die Relevanz für Gesundheit haben. Bei Mobilgeräten ist die genutzte Sensorik in der Praxis oft nur eingeschränkt aussagekräftig für die zu erhebenden körperlichen Merkmale. Sie haben auch keine sichere Aussagekraft zum Aufenthaltsort einer Person, da Mobilgeräte an andere Person weitergegeben oder abgelegt werden können. Bei der Feststellung von ansteckungsrelevanten Kontakten kommt es darauf an, wie räumlich präzise und wie zeitlich intensiv diese sind. Ungeeignet sind hierzu Funkzellenzuordnungen, aber zumeist auch GPS-Daten, da diese zumeist nur zweidimensionale Aussagen erlauben. Digital schwer erfassbar sind Umstände zu Schutzmaßnahmen (Masken, Kleidung) und Kontexten (drinnen/draußen, Krankenhaus, Supermarkt, Restaurant), die für die Aussagekraft von Daten oft von zentraler Bedeutung sind. Der Grundsatz der Datenrichtigkeit verpflichtet zur Abbildung dieser Unwägbarkeiten, etwa indem berücksichtigt wird, ob und inwieweit nur Wahrscheinlichkeits- bzw. Risikoaussagen gemacht werden.

Der Grundsatz der *Speicherbegrenzung* (Art. 5 Abs. 1 lt. E DSGVO) sieht vor, dass identifizierende Daten nur solange gespeichert werden dürfen, wie es für den Verarbeitungszweck erforderlich ist. Bei einer Sekundärnutzung für wissenschaftliche Zwecke ist, wenn geeignete technisch-organisatorische Maßnahmen zum Einsatz kommen, eine längere Speicherung erlaubt. D.h. nach Zweckerreichung sind die zuordnenden Probandendaten zu löschen oder zumindest zu anonymisieren (Art. 17 Abs. 1 lit. a, Abs. 3 lit. d DSGVO). Gerade im Hinblick auf die Löschpflicht ist eine präzise Beschreibung des Verarbeitungszwecks dringend nötig. So besteht weitgehend Einigkeit, dass per Bluetooth erfasste Kontaktdaten zum Zweck der Warnung vor einer möglichen Infektion angesichts der Inkubationszeit und der nötigen Zeit zur Feststellung und Kommunikation einer Infektion spätestens nach 14 Tagen gelöscht werden können und müssen.

Hinsichtlich der *Integrität und Vertraulichkeit* (Art. 5 Abs. 2 lit. f DSGVO) kommen im Interesse der technisch-organisatorischen Sicherheit (Art. 32 DSGVO, § 22 Abs. 2 BDSG) weitere Aspekte hinzu: Wo werden Daten gespeichert bzw. abgeglichen: dezentral oder zentral, auf dem Gerät des Betroffenen oder auf einem Server eines Hintergrundsystems? Welche Formen der Verschlüsselung und der Pseudonymisierung werden gewählt? Welche Missbrauchsrisiken sind mit bestimmten technischen Verfahren, etwa dem Bluetooth-Einsatz, verbunden? Wird und wie wird verhindert, dass Plattform-, Hardware- und Software-Anbieter auf die Daten einer konkreten Corona-Anwendung Zugriff nehmen können? Durch die Technikgestaltung muss eine weitestgehende Datenminimierung erreicht werden (Art. 25 Abs. 1, 2 DSGVO).

23 Der Nutzen von Warn-Apps

Angesichts der vielen Unwägbarkeiten gibt es Stimmen, die schon die *Geeignetheit* von App-Anwendungen zur Coronabekämpfung in Frage stellen. App-Warnungen sind für die Betroffenen nur sinnvoll, wenn diesen daraufhin wirksame Schutzmaßnahmen möglich sind. Schutzmaßnahmen sind auch ohne App möglich und dringend zu empfehlen. So sind die Beachtung von Distanzgeboten oder die Atemschutzmaskennutzung unabhängig von digitalen Maßnahmen. Durch digitale Warnungen ausgelöste Schutzmaßnahmen sollen darin bestehen, dass frühzeitig ein Test durchgeführt wird. Im Fall eines positiven Befundes können präventive Behandlungsmaßnahmen ergriffen werden sowie Vorkehrungen zur Vermeidung weiterer Infektionen. Tests können aber nicht die Infektion verhindern.

Angesichts fehlender Behandlungsmöglichkeiten bei einer SARS-CoV-2-Infektion ist der individuelle *Nutzen für den Betroffenen* selbst eingeschränkt. Der hauptsächliche Nutzen liegt darin, dass weitere Infektionen vermieden und dadurch Andere geschützt werden. Ermöglicht eine Corona-App es tatsächlich Infektionswege nachzuvollziehen, so sind diese Informationen aus wissenschaftlicher Sicht von Bedeutung. Das Nachvollziehen von Infektionswegen wird aber bei Vielfachmeldungen aufgrund einer massenhaften Durchseuchung wieder schwierig oder gar unmöglich.

Aussagen zur Geeignetheit lassen sich nicht pauschal machen. Vielmehr bedarf es einer *präzisen Prüfung* der eingesetzten Technik in Hinblick auf die konkret verfolgten Ziele zu einem bestimmten Zeitpunkt in einer bestimmten Umgebung unter Berücksichtigung vieler externer Aspekte. Solche Aspekte können auch im ökonomischen und psychischen Bereich liegen. Die Rate der Anwendungsverweigerer oder Nichtnutzer sowie deren soziale Zusammensetzung können Auswirkungen auf die Geeignetheit haben.

Corona-Apps sollen eine „systematische und umfassende Bewertung persönlicher Aspekte" ermöglichen, indem eine „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten" erfolgt und dies erfolgt durch eine „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche". Nutzen und Risiken derartiger Anwendungen müssen deshalb in jedem Fall einer Datenschutz-Folgenabschätzung zugeführt werden (Art. 35 Abs. 3 DSGVO).[51] Die informationellen Maßnahmen gegen Covid-19

sollten zudem regelmäßig nach kurzen Zeiträumen einer Evaluation unterworfen werden.

24 Gesetzgebungsbedarf

Der Einsatz von digitalen Instrumenten zur Eindämmung von Covid-19 ist voraussetzungsvoll und von Unwägbarkeiten begleitet. Es besteht aber mit der DSGVO ein *valider Rechtsrahmen*, mit dem auf freiwilliger Basis unterstützende Maßnahmen durchgeführt werden können.[52] Bei diesen Maßnahmen muss verhindert werden, dass der freiheitliche Charakter unserer gesellschaftlichen Ordnung verlassen wird. Autoritäre Bestrebungen finden in Krisenzeiten schnell Gehör – auch bei uns in Deutschland.

Auch wenn der allgemeine Rahmen ausreichend erscheint, so besteht bzgl. der *spezifischen Regulierung* Diskussionsbedarf. Falsch ist die Forderung des Deutschen Ethikrats, angesichts der bestehenden gesundheitlichen Herausforderungen die Anforderungen an Zweckbindung und Datenminimierung herunterzufahren, um dann mit Hilfe von Big Data und sog. Künstlicher Intelligenz neue Antworten geben zu können.[53] Das Infektionsschutzgesetz bietet, soweit dies nach den bisherigen Erfahrungen beurteilt werden kann, einen validen Rahmen für die notwendigen informationellen Maßnahmen zum Umgang mit Pandemien.

Ein rechtliches Einfallstor für Vertraulichkeit und Zweckbindung von personenbezogenen Gesundheitsdaten besteht derzeit, wenn Daten *von den Betroffenen selbst bereitgestellt* werden. Dies beginnt mit der Vertrauenswürdigkeit der IT-Verfahren. Die im SGB V in § 33a vorgesehenen Instrumente zur Bewertung von digitalen Gesundheitsanwendungen sind ungenügend. Die in der DSGVO vorgesehenen Möglichkeiten zur Zertifizierung sind noch nicht in der Praxis angekommen. Die ärztliche Schweigepflicht, mit der eine gesundheitsbezogene Zweckbindung hergestellt werden könnte, gilt bei diesen Anwendungen bisher nicht oder nur eingeschränkt.

Entsprechendes gilt für die freiwillige Bereitstellung von Gesundheitsdaten für die *medizinische Forschung*. So ist für die dem RKI von Betroffenen per „Datenspende“ über Gesundheits-Apps bereitgestellten Daten trotz der ärztlichen Leitung des RKI das Patientengeheimnis in Form der ärztlichen Schweigepflicht nicht anwendbar. Nötig wäre daher eine umfassende gesetzliche Etablierung eines Forschungsgeheimnisses, das Forschungsdaten von der Beschlagnahme für Strafverfolgungszwecke freistellt.

Der „Sachverständigenrat Gesundheit“, ein Gremium, das die Politik in gesundheitspolitischen Fragen berät, nahm die Corona-Pandemie zum Anlass, eine verstärkte *Digitalisierung des Gesundheitswesens* zur fordern. Wäre Deutschland weiter, etwa bei der Einführung einer elektronischen Gesundheitsakte, bei der Telemedizin oder beim Datenaustausch über Gesundheitsnetze, „könnten wir längst mehr über Covid-19 wissen und so Menschenleben retten“.[54] So richtig die Forderung ist, so falsch ist die Begründung: Die Pandemie hat auch hochdigitalisierte Staaten von hinten erwischt. Bei einer Krankheit, über die – wie bei Covid-19 – zunächst nichts bekannt ist, kann Digitalisierung allenfalls einen begrenzten Beitrag leisten zu einem umfangreichen Maßnahmebündel. Im hochdigitalisierten Südkorea wurden mit MERS Erfahrungen gesammelt, die bei der Eindämmung von SARS-CoV-2 zugrunde gelegt wurden. Aus der aktuellen Pandemie können Lehren gezogen werden. Die wirksamen Gegenmaßnahmen sind bisher vor allem medizinische oder analog körperliche – vom Maskentragen und Abstandswahren bis hin zur Testung, Untersuchung und Behandlung. Diese können auch digital sein. Bei diesen Maßnahmen muss jeweils geprüft werden, inwieweit hierbei Grundrechtseingriffe erfolgen und inwieweit deshalb gesetzliche Grundlagen mit Sicherheitsvorkehrungen nötig sind.

Wir befinden uns mitten in der Corona-Pandemie. Aus Datenschutzsicht ist erhöhte Aufmerksamkeit geboten. Zugleich sollten aber auch nicht aus grundsätzlichen Erwägungen des Bürgerrechtsschutzes *sinnvolle Datenerhebungen und -auswertungen* be- und verhindert werden. Wir brauchen dafür den Dialog zwischen allen Beteiligten, nicht das Sichverschanzen in überkommenen Rollen.

1 Schumann, Wie eine Smartphone-App aus Deutschland vor Ebola schützen soll, www.tagesspiegel.de 30.10.2019.

2 Giesen, Dem Algorithmus unterworfen, SZ 26.03.2020, 7; Deuber, Der ganz normale Ausnahmezustand, SZ 25./26.04.2020, 9.

3 Däubler, Corona-Virus und Datenschutz, CuA 4/2020, 25 f.

4 Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (Bock/Kühne/Mühlhoff/Ost/Pohle/Rehak), Datenschutz-Folgenabschätzung für die Corona-App, Version 1.3 v. 17.04.2020 (künftig zitiert mit FIfF, En. 4), S. 16.

5 Zand, Der große Angriff, Der Spiegel Nr. 12 v. 14.03.2020, 68 f.

6 Peters, Ein Land wird getestet, Der Spiegel Nr. 15 v. 04.04.2020, 86; Hahn, Die Kunst der Übertreibung, SZ 17.04.2020, 3.

7 Beuth/Höflinger/Knobbe/Rojkov/Rosenbach/Schindler, Programmiertes Chaos, Der Spiegel Nr. 18 v. 25.04.2020, 25.

8 FIfF, En. 4, S. 16.

9 Avenarius/Bigalke/Dörries/Föderl-Schmid/Reuss, Verlockungen des Ausnahmezustands, SZ 09./10.04.2020, 9; Föderl-Schmid, Geheimdienst soll Infizierte aufspüren, SZ 21./22.03.2020, 9.

10 Einen Überblick zu allen EU-Staaten (Stand Mitte April) findet sich bei eHealth Network, Mobile applications to support contact tracing in the EU´s fight against Covid-19 – Common EU Toolbox for Member States Version 1.0 v. 15.04.2020, S. 10-12.

11 Baumstieger/Beisel/Föderl-Schmid/Grossmann/Hahn/Hassel/Hurtz, Schöne neue Welt, SZ 07.04.2020, 7; Beuth/Höflinger/Knobbe/Rojkov/Rosenbach/Schindler, Programmiertes Chaos, Der Spiegel Nr. 18 v. 25.04.2020, 27.

12 FIfF, En. 4, S. 16; Krempl, Stopp-Corona-App: Österreich will Vorzeigemodell für Europa schaffen, www.heise.de 22.04.2020.

13 Recommendation of 8 April 2020 on a common Union Toolbox of technology on data to combat and exit from Covid-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data (C(2020) 2296 final).

14 Joint European Roadmap towards lifting Covid-19 containment measures (nicht datiert).

15 Edpd, Guidelines 04/2020 on the use of location data und contact tracing tools in the context of the Covid-19 outbreak, 21.04.2020; Ermert, EU-Datenschützer: Richtlinien für datengestützte Pandemie-Bekämpfung, www.heise.de 22.04.2020.

16 Herrmann, Hier spricht das Gesundheitsamt, SZ 27.04.2020, 3.

17 Schulzki-Haddouti, Medizinische Hochschule und Ubilabs entwickeln Corona-App, www.heise.de/-4680487 v. 11.03.2020.

18 Dalg, RKI bekommt Handydaten von Deutscher Telekom, www.tagesspiegel.de 18.03.2020; Telekom gibt Bewegungsdaten an das Robert-Koch-Institut weiter, www.handelsblatt.com 18.03.2020.

19 Schwan, SARS-CoV-2: Apple stellt Bewegungsdaten zur Verfügung, www.heise.de 15.04.2020.

20 Gesetz v. 27.03.2020, BGBl. I v. 27.03.2020, S. 587.

21 Bartsch/Friedmann/Gebauer/Gude/Hackenbroch/Latsch/Schmundt/Winter, Kein Exit, Der Spiegel Nr. 15 04.04.2020, 40.

22 Appel, Verwirrung und Täuschung mit Corona-APPs, extradienst.net 12.04.2020.

23 Schäfer, Covid-19: Corona-App weist Sicherheitslücke auf, www.e-recht.de 06.04.2020; einen umfassenden Überblick enthält Tagesspiegel Background Digitalisierung & KI 28.04.2020.

24 https://covapp.charite.de/.

25 App soll Quarantäne überwachen, www.tagesspiegel.de Background Digitalisierung & KI 21.04.2020.

26 Hurtz/Janisch, Mit Buetooth gegen Corona, SZ 31.03.2020, 5.

27 Krempl, EU-Kommission will Wildwuchs bei Corona-Apps verhindern, www.heise.de 09.04.2020.

28 eHealth Network, Mobile applications to support contact tracing in the EU´s fight against Covid-19 – Common EU Toolbox for Member States Version 1.0 v. 15.04.2020.

29 European Data Protection Board (EDPB), Brief an den Head of Unit European Commission DG Justice and Consumers Unit C.3 v. 14.04.2020.

30 Schulzki-Haddouti, Corona-Tracking-Apps mit PEPP-PT: „Entscheidend ist für uns, dass der Datenschutz gewährleistet wird“, www.heise.de/-4700336 09.04.2020; Baumstieger/Beisel/Föderl-Schmid/Grossmann/Hahn/Hassel/Hurtz, Schöne neue Welt, SZ 07.04.2020, 7.

31 Tangens/Büschke, Die neue „Corona-App“ – Eine Einordnung von Digitalcourage, digitalcourage.de 08.04.2020, weisen darauf hin, dass bei Android der Einsatz von Bluetooth bisher zwingend mit der Erfassung von Ortsdaten kombiniert war.

32 www.media.mit.edu/projects/safepaths/overview/.

33 Hurtz/Muth, Pakt der Rivalen, SZ 15.04.2020, 19; Becker, Coronavirus: Kontaktverfolgung wird Teil von Android und iOS, www.heise.de 14.04.2020.

34 Schulzki-Haddouti, PEPP-PT-Projekt: Forscher fordern besseren Datenschutz bei Corona-Warn-Apps, www.heise.de 20.04.2020; Krempl, Kontakt-Tracing vs. Corona: Aderlass beim Pilotprojekt PEPP-PT geht weiter, www.heise.de 20.04.2020; Hurtz, App zum Ärgern, SZ 21.04.2020, 5.

35 Corona-Tracing-App: Offener Brief an Bundeskanzleramt und Gesundheitsminister, www.ccc.de 24.04.2020.

36 Tracing Apps, Tagesspiegel Digitalisierung & KI Background 28.04.2020 u. 29.04.2020, Hurtz, Tagebuch der Kontakte, SZ 28.04.2020, 2; Krempl, Dezentrale Lösung: Bundesregierung sattelt bei Corona-Tracing-App radikal um, www.heise.de 26.04.2020.

37 Zielcke, Pademie-Absolutismus, SZ 17.04.2020, 13.

38 Krempl, Corona-Maßnahmen: Snowden warnt vor „Architektur der Unterdrückung“, www.heise.de 11.04.2020.

39 Siehe dazu die aktuellen Entscheidungen des BVerfG: B. v. 15.04.2020 – 1 BvR 828/20, B. v. 10.04.2020 – 1 BvQ 28/20, B. v. 07.p4.2020 – 1 BvR 755/20, PM Nr. 23/2020 v. 08.08.2020, Erfolglose Eilanträge im Zusammenhang mit der Covid-19-Pandemie.

40 BVerfG 15.12.1983 – 1 BvR 209/83 u.a. (Volkszählung), Rn. 94, NJW 1984, 422; BVerfG 12.04.2005 – 2 BvR 1027/02 (Beschlagnahme Anwaltskanzlei), Rn. 70, NJW 2005, 1918.

41 Baum/Bäumer u.a., Corona-Pandemie bekämpfen, Bürgerrechte und Datenschutz wahren! 02.04.2020, https://www.eaid-berlin.de/appell-der-europaeischen-akademie-fuer-informationsfreiheit-und-datenschutz-corona-pandemie-bekaempfen-buergerrechte-und-datenschutz-wahren/.

42 Leopoldina, Dritte Ad-hoc-Stellungnahme: Corona-Pandemie – Die Krise nachhaltig überwinden, 13.04.2020, S. 7.

43 Gesetz vom 20.07.2000, BGBl. I S. 1045, zuletzt geändert durch Gesetz v. 27.03.2020, BGBl. I S. 587.

44 FIfF, En. 4, S. 32 ff.

45 Schuler, Was heißt hier „anonym“? www.netzwerk-datenschutzexpertise.de 16.04.2020.

46 Kugelmann, a.A. Thüsing, abwägend Schwartmann, alle: Freiwillig oder mit Zwang? www.faz.net 04.09.2020.

47 Gössner, Gedanken und Thesen zum Corona-Ausnahmezustand, Ossietzky v. 18.04.2020, S. 3.

48 Schuler, Was heißt hier „freiwillig“? www.netzwerk-datenschutzexpertise.de 27.04.2020.

49 EDPB, Brief an den Head of Unit Enit European Commission DG Justice and Consumers v. 14.04.2020; kritisch FIfF, En. 4, S. 54 f.

50 Tangens/Büschke, Die neue „Corona-App“ – Eine Einordnung von Digitalcourage, digitalcourage.de 08.04.2020.

51 Vgl. FIfF, En. 4; vgl. Chaos Computer Club, 10 Prüfsteine für die Beurteilung von „Contact Tracing“-Apps, www.ccc.de 06.04.2020.

52 A.A. FIfF, En. 4, S. 85, das eine gesetzliche Regelung für den APP-Einsatz fordert.

53 Deutscher Ethikrat, Big Data und Gesundheit, Datensouveränität als informationelle Freiheitsgestaltung, 2017, u.a. S. 22 f.; dagegen richtig Kühling DuD 2020, 182 ff.

54 Gerlach/Greiner/Jochimsen/von Kalle/Meyer/Schreyögg/Thürmann, Daten teilen – besser heilen, www.spiegel.de 21.04.2020.

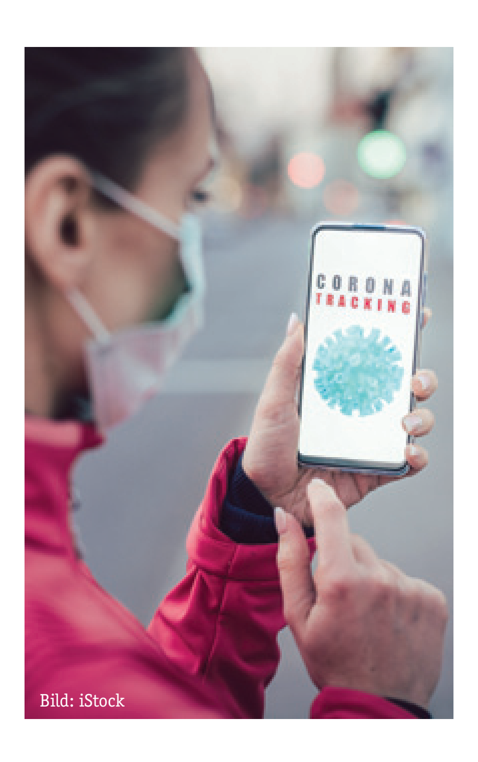


Bild: iStock

Kirsten Bock, Christian Ricardo Kühne, Rainer Mühlhoff, Měto R. Ost, Jörg Pohle, Rainer Rehak

Tracing-Apps datenschutzfreundlich gestalten und betreiben

Die Datenschutz-Folgenabschätzung als Diskussionsermöglicher und Gestaltungsinstrument

Abstract:

Mit der Entwicklung und dem Einsatz von Tracing-Apps für die Verfolgung von CoV-2-Infektionen werden einerseits große Hoffnungen bei der Pandemiebekämpfung verbunden, andererseits Befürchtungen um massive Grundrechtsgefährdungen. Artikel 35 DSGVO verlangt von Verantwortlichen, dass sie eine Datenschutz-Folgenabschätzung (DSFA) durchführen, wenn ihre Datenverarbeitung wahrscheinlich zu einem hohen Risiko für die Grundrechte und -freiheiten führt. Eine DSFA ist eine strukturierte Risikoanalyse, die mögliche grundrechtsrelevante Folgen der Datenverarbeitung im Voraus identifiziert und bewertet sowie Maßnahmen zur Minimierung dieser Risiken beschreibt oder darstellt, dass die Risiken nicht minimiert werden können.

WissenschaftlerInnen und DatenschützerInnen im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. haben eine DSFA für Tracing-Apps vorgelegt, um eine öffentliche Debatte über die damit einhergehenden Risiken für Grundrechte und -freiheiten anzustoßen und zu informieren. Der vorliegende Beitrag beleuchtet die Hintergründe und erklärt die Wahl der Form einer DSFA für die Intervention in die gesellschaftliche Debatte. Auf zwei für die datenschutzrechtliche Debatte besonders relevante Aspekte wird anschließend näher eingegangen: auf die Unterscheidung zwischen Freiwilligkeit und Einwilligung sowie auf das Problem von Personenbezug und Anonymisierung. Die vorgelegte DSFA setzt einen technischen, rechtlichen und methodischen Maßstab dafür, wie in Zukunft die Funktionen von Verarbeitungsverfahren und die daraus sich ergebenden Datenschutzrisiken für Betroffene und die Gesellschaft zu analysieren, zu bestimmen und gegebenenfalls zu verringern sind.

Seit der Ausbreitung des SARS-CoV-2-Virus in Europa Anfang 2020 wird der Ruf nach technischen Lösungen lauter, die bei der Bekämpfung oder Eindämmung der Pandemie zum Einsatz kommen sollen. Im Zentrum der Debatten stehen Tracing-Apps, die aufgrund der globalen Verbreitung von Smartphones mit der Verheißung aufgeladen werden, die herkömmlichen Verfahren zur Erforschung des epidemiologischen Verlaufs zu unterstützen. Diese Systeme würden automatisiert die zwischenmenschlichen Kontakte aller NutzerInnen aufzeichnen und es so erlauben, die Infektionsketten des Virus schnell und effizient – auch rückwirkend – nachzuvollziehen, um möglicherweise exponierte Personen frühzeitig isolieren zu können. Unter den verschiedenen eingesetzten Systemen und Systementwürfen stechen jene hervor, die damit werben, den Anforderungen der DSGVO zu entsprechen. Die DSGVO selbst verpflichtet die BetreiberInnen umfangreicher Datenverarbeitungssysteme, zu denen auch solche Tracing-Apps in jedem Fall zählen, zur Anfertigung einer Datenschutz-Folgenabschätzung (DSFA) aufgrund des hohen Risikos für die Grundrechte und -freiheiten (Art. 35 DSGVO). Bei einer DSFA handelt es sich um eine strukturierte Risikoanalyse, die mögliche grundrechtsrelevante Folgen einer Datenverarbeitung im Vorfeld identifiziert und bewertet, Maßnahmen beschreibt, mit denen diese Risiken adressiert werden sollen, oder darstellt, dass und warum es solche Maßnahmen im konkreten Fall nicht gibt oder geben kann.

Nur für ein einziges derzeit eingesetztes oder in der Entwicklung befindliches System zur Kontaktverfolgung hat die entsprechende BetreiberIn bisher eine solche DSFA öffentlich zur Verfügung gestellt.[1] Zwar hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Ulrich Kelber, am 8. April 2020 auf Twitter erklärt, seiner Behörde sei eine DSFA für die „Datenspende"-App des Robert-Koch-Instituts (RKI) vorgelegt worden,[2] aber weder ist diese öffentlich gemacht worden noch gibt es Informationen über den Prüfumfang oder die Prüftiefe.

Vor diesem Hintergrund hat sich eine Gruppe WissenschaftlerInnen und DatenschützerInnen im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. zusammengefunden, um eine DSFA für Corona-Apps auszuarbeiten (Bock et al. 2020). In diesem kurzen Beitrag wollen wir die Hintergründe beleuchten und erklären, warum wir für unsere Intervention die Form einer DSFA gewählt haben. Anschließend werden wir zwei Aspekte herausgreifen, die uns als für die datenschutzrechtliche Debatte besonders relevant erscheinen: erstens die Unterscheidung zwischen Freiwilligkeit und Einwilligung und zweitens das Problem von Personenbezug und Anonymisierung.

Die DSFA als Diskussionsermöglicher und Gestaltungsinstrument

Wir haben es angesichts der geplanten Corona-Tracing-Systeme mit einem gesellschaftlichen Großexperiment zur digitalen Verhaltenserfassung unter

staatlicher Aufsicht in Europa zu tun. Wirksamkeit und Folgen entsprechender Apps sind bislang allenfalls teilweise absehbar, nicht zuletzt weil viele Eigenschaften, darunter selbst ihre Zwecke, nicht abschließend ausgehandelt sind. Dennoch ist bereits deutlich, dass die datenschutz- und somit grundrechtsrelevanten Folgen dieses Großexperiments nicht nur Einzelpersonen, sondern die Gesellschaft als Ganze betreffen. Aus diesem Grunde ist nicht nur die Anfertigung einer DSFA angezeigt, sondern insbesondere auch ihre Veröffentlichung – und eine öffentliche Diskussion. Eine solche gesellschaftliche Diskussion voranzutreiben, nicht nur in Deutschland, sondern in Europa insgesamt, war eines der Ziele, die wir mit der Veröffentlichung der Datenschutz-Folgenabschätzung auf Deutsch, Englisch, Französisch und Spanisch verfolgt haben.

Wir haben dabei zweitens die Form einer DSFA gewählt, weil sie einem Aufbau folgt, der die für eine öffentliche Diskussion notwendigen Informationen strukturiert und zugleich umfassend darzustellen erlaubt. Als methodologische Grundlage haben wir dazu das Standard-Datenschutzmodell (SDM) in der Fassung V2.0a, das im November 2019 von der 98. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder beschlossen wurde, verwendet. Damit gelingt es, nicht allein die grundrechtsrelevanten Folgen einer Datenverarbeitung zu identifizieren, sondern auch darzustellen, auf welchen Annahmen diese Risikoanalyse basiert: Annahmen über AkteurInnen, ihre Eigenschaften und Interessen, die dann als AngreiferInnen auf Grundrechte auftreten können, über das Verarbeitungsverfahren und seinen Zweck und über die technischen Systeme, die in dieses Verfahren eingebettet sind. Erst diese Offenlegung ermöglicht eine informierte gesellschaftliche Debatte.

Und drittens soll die von uns vorgelegte DSFA als Maßstab für alle zukünftigen DSFAen dienen. So soll verhindert werden, dass mit Hilfe von defizitären oder gar „Marketing-DSFA" (Friedewald et al. 2016: 21) Betroffenen und Aufsichtsbehörden die Risikolosigkeit einer Technologie oder eines Systems verkauft wird, indem mit geringem Aufwand eine DSFA durchgeführt wird, die auf engen Systemdefinitionen, intransparenten Kriterien für Risikoidentifikation und -bewertung und einer Gleichsetzung von Kriterien der Informationssicherheit mit denen des Datenschutzrechts basiert.

An der einen oder anderen Stelle haben wir gegenüber einer „klassischen" DSFA nach Art. 35 DSGVO kleinere Änderungen bei der Struktur und der Darstellungstiefe vorgenommen, die sich aus dem Charakter der vorliegenden DSFA als „Gestaltungs-DSFA" ergeben. Die wichtigsten vorliegenden Entwürfe befanden sich zum Zeitpunkt der Durchführung teils noch in einem frühen Entwicklungsstadium, wobei teilweise zentrale Aspekte noch nicht geklärt waren, die der europäische Verordnungsgeber aber offensichtlich bei der Niederlegung der Anforderungen in Art. 35 DSGVO als zum Durchführungszeitpunkt gegeben angenommen und vorausgesetzt hat. So war noch nicht geklärt, welche Organisation für die Gestaltung und den Betrieb einer Verarbeitung mit Hilfe einer Tracing-App, wenn sie denn realisiert wird, verantwortlich sein wird.[3] Ebenso wenig war die rechtliche und die funktionale Ausgestaltung der Datenverarbeitung festgelegt.[4] Für die untersuchte Datenverarbeitung hat das zur Folge, dass im Rahmen der DSFA die Konkretisierung selbst zum Gegenstand gemacht und damit gestaltet werden kann. Die Datenverarbeitung wurde dabei von den AutorInnen in einem rekursiven Prozess des wechselseitigen Aufeinander-Beziehens von rechtlichen, organisatorischen und technischen Kriterien dergestalt entwickelt, dass sie im Urteil der AutorInnen den Zweck funktional vollumfänglich erfüllt und dabei im geringst möglichen Umfang in die Rechte und Freiheiten von Personen eingreifen würde, wobei der Zweck im Rahmen dieses Prozesses selbst auch geschärft und erst am Ende als Zweck im datenschutzrechtlichen Sinne gesetzt wurde (vgl. Pohle 2018: 271, Fn. 163). Anschließend werden für diesen Zweck die möglichen Auswirkungen im Hinblick auf die Relevanz der identifizierten Risiken (Validität), die Wirksamkeit der Maßnahmen und deren Belastbarkeit (Reliabilität) antizipiert. Eine „Gestaltungs-DSFA" in dieser Form macht nicht nur die Zwecksetzung selbst zum diskutierbaren Teil der das System definierenden Vorentscheidungen der Verantwortlichen, sie erlaubt gerade auch, dass nicht nur einzelne Details, sondern alle Aspekte der Verarbeitung grundrechtsfreundlich gestaltet werden können, und hilft damit die Anforderungen von Art. 24 und Art. 25 DSGVO – Accountability und Datenschutz by Design – zu erfüllen.

Ganz wesentlich für eine DSFA nach der DSGVO ist, dass nicht eine hervorstechende Technik, in diesem Falle die Corona-App, in den Fokus gestellt wird. Im Fokus der DSFA steht stattdessen das Verfahren insgesamt, das aus mehreren personenbezogenen Verarbeitungstätigkeiten besteht, in denen selbst wieder Vorgänge oder Vorgangsreihen stattfinden oder vorgenommen werden – teilweise technikgestützt. Die Betrachtung muss also über die Nutzung der App hinausgehen, denn die Grenze der App ist nicht die Grenze der Verarbeitung.

Ebenso wesentlich ist eine umfassende Kontextierung. Nicht nur hilft sie bei der Identifizierung der möglichen AngreiferInnen und der Konkretisierung der Zwecke, sie ist vor allem erforderlich für die rechtliche Abwägung im Rahmen der Verhältnismäßigkeitsprüfung nach Art. 35 Abs. 7 lit. b DSGVO.

Freiwilligkeit und Einwilligung

In Bezug auf die Nutzung der App fallen üblicherweise die Begriffe Freiwilligkeit und Einwilligung, die jedoch oft vermischt werden. Dabei bezeichnet der erste Begriff den Umstand, ob Personen sich selbst entscheiden können, die App zu nutzen oder aber ob die Nutzung der App vorgeschrieben ist, sie also zwangsweise von allen genutzt werden muss. Beim zweiten Begriff der Einwilligung geht es konkret um die datenschutzrechtliche Frage, auf welcher Rechtsgrundlage die Datenverarbeitung stattfinden soll. Bei einer Einwilligung wird der BenutzerIn vorgelegt, welche Datenverarbeitung die App und das dahinter liegende System innerhalb des Datenverarbeitungsverfahrens genau vornimmt, und dann eine Zustimmung dafür eingeholt. Insofern diese Entscheidung gem. Art. 4 Nr. 11 DSGVO informiert, spezifisch, aktiv und unbeeinflusst getroffen wird, gilt sie rechtlich als Einwilligung (Art. 6 Abs. 1

lit. a, Art. 7 DSGVO). Es gibt jedoch auch andere Rechtsgrundlagen für eine Datenverarbeitung, etwa die Erforderlichkeit der Datenverarbeitung für die Erfüllung eines Vertrages (Art. 6 Abs. 1 lit. b DSGVO) oder aber auf Basis eines Gesetzes (Art. 6 Abs. 1 lit. e DSGVO).

Die Freiwilligkeit der App-Nutzung ist dabei unabhängig von der datenschutzrechtlichen Rechtsgrundlage für das Verfahren insgesamt zu sehen. Zwar kann es keine Zwangs-App mit Einwilligung geben, jedoch ist eine freiwillige App mit einer gesetzlichen Grundlage denkbar, ja sogar wünschenswert. Sie ist deswegen wünschenswert, weil bei einer Einwilligungslösung die Verantwortliche für das Verfahren und BetreiberIn der App allein entscheidet, worin genau die NutzerInnen einwilligen sollen. Gerade auch in der vorliegenden Konstellation, in der die App nur genau so operiert, wie von der Verantwortlichen vorgegeben, und damit, obzwar sie auf dem Smartphone der Betroffenen läuft, ausschließlich unter der Kontrolle der Verantwortlichen, vergleichbar zu einem DRM-System (Becker et al. 2003), wird gleichzeitig das Risiko einer Abwägung der Grundrechtsrisiken gegenüber der Zweckerreichung auf die Betroffenen externalisiert (Rost 2018) – die durch die Verarbeitung verursachte informationelle Machtasymmetrie zwischen der Verantwortlichen und der Betroffenen wird so nicht nur nicht ausgeglichen, sondern verstärkt. Mit dem Robert Koch-Institut als Verantwortlichem, einer deutschen Bundesoberbehörde, ist es ohnehin höchst fragwürdig, wie frei Personen in ein solches BürgerIn-Staat-Verhältnis einwilligen können.

Bei einer freiwilligen App auf Basis einer gesetzlichen Grundlage hingegen würde direkt die (demokratisch legitimierte) GesetzgeberIn die Verarbeitung festlegen und deren Grenzen definieren. Dafür käme beispielsweise eine Erweiterung des Infektionsschutzgesetzes (IfSG) in Betracht. Zudem ist zu beachten, dass die DSGVO nach Art. 89 eine weitreichende Nutzung vorhandener Daten zu Forschungszwecken ermöglicht. Bei einer gesetzlichen Grundlage für die Datenverarbeitung können auch dafür die genauen Zwecke expliziert oder aber nach einer negativen Verhältnismäßigkeitsprüfung derartige Weiternutzungen explizit verboten werden.

Vor dem Hintergrund dieser Überlegungen ist eine freiwillige App auf Basis einer gesetzlichen Grundlage sowohl aus Datenschutzsicht wünschenswert als auch rechtlich geboten. Darüber hinaus müsste flankierend eine weitere Rechtsvorschrift die Zweckentfremdung der App – als Zugangserlaubnis für Gebäude oder Arbeitsstellen – untersagen. Dies ist einerseits nötig, um die Nutzung der App nicht nur de lege, sondern auch de facto freiwillig zu machen, sowie um andererseits die Zweckerreichung zu unterstützen. Sollte sich nämlich andeuten, dass die App-gestützte Risikoprognose zu schwerwiegenden Nachteilen im täglichen Leben führt, so würden die NutzerInnen schnell Wege finden, die App vor Risikosituationen zu deaktivieren. In der Folge würde die App ihren Zweck nicht mehr erfüllen können – sie wäre nicht mehr geeignet und demnach nicht mehr zulässig.

Personenbezug und Anonymisierung

In der Diskussion um die Eigenschaften einer Corona-App wird häufig von einem „anonymen System“ gesprochen, teilweise wird deswegen sogar die Anwendung der DSGVO an sich in Frage gestellt. Die Funktionalität der App wird umgesetzt, indem sie in regelmäßigen Abständen wechselnde Zeichenfolgen via Bluetooth versendet und entsprechend die Zeichenfolgen von anderen Apps empfängt, sofern diese örtlich nah genug sind. Versendete und empfangene Zeichenfolgen werden getrennt gespeichert. Wenn eine NutzerIn nun positiv getestet wird, so lädt sie in der datensparsamen Variante der App ihre gesendeten Zeichenfolgen auf den Server, wonach andere Apps diese von dort erhalten, um prüfen zu können, ob sie selbst Kontakt mit Infizierten hatten. Das Verfahren besteht insgesamt also aus der Verarbeitung von Kontaktdaten auf den Smartphones, der Übermittlung dieser Daten auf einen Server nach der Diagnose einer Infektion und letztendlich deren Verteilung an alle anderen Smartphones zur Prüfung auf einen möglichen Kontakt mit Infizierten. Alle Daten auf einem Smartphone sind direkt personenbezogen, nämlich bezogen auf die NutzerIn des Gerätes. Dies gilt unabhängig davon, ob das Gerät gut nach außen abgesichert ist oder inwiefern andere Apps die empfangenen Zeichenfolgen direkt einer Person zuordnen können, prinzipiell möglich ist es allemal. Und weil nur diejenigen Personen Daten an den Server übertragen, die als infiziert diagnostiziert wurden, sind die übertragenen Daten zugleich Gesundheitsdaten, also besondere Arten von personenbezogenen Daten nach Art. 9 DSGVO.

An dieser Stelle werfen wir ein besonderes Augenmerk auf das gebotene Anonymisierungverfahren beim Upload der Daten auf den Server. Bei einem ungeschützten Verfahren könnte die BetreiberIn des Servers prinzipiell über die IP-Adresse der hochladenden App einen Personenbezug herstellen, die Daten also re-personalisieren und sogar die Infektion zuschreiben. Dieser Personenbezug muss also beim Hochladevorgang von den versendeten Zeichenfolgen zuverlässig abgetrennt werden, damit diese vom Server verarbeitet und an andere Apps weiterverbreitet werden kann. Anschließend handelt es sich nur noch „infektionsanzeigenden Daten ohne Personenbezug“. In diesem Trennungsprozess wird demnach die Identifizierbarkeitsrelation aufgehoben, ohne dass sich der Informationsgehalt der Daten selbst oder ihre Nutzbarkeit für den angestrebten Zweck ändern (vgl. Art. 29 WP 2007).

Dieses Anonymisierungverfahren kann konkret vielgestalt aussehen, wobei stets auf kontinuierliche Prüfbarkeit geachtet werden muss. Das Verfahren muss jedoch immer durch eine Kombination aus rechtlichen, technischen und organisatorischen Maßnahmen abgesichert werden (Podlech 1976) und kontinuierlich datenschutzrechtlich durch die zuständige Aufsichtsbehörden prüfbar sein. Rechtlich muss die BetreiberIn unabhängig sein und keine eigenen Interessen an den Daten haben dürfen. Sie muss zudem vor Pflichten zur Herausgabe von Daten geschützt sein, auch gegenüber staatlichen Sicherheitsorganen. Organisatorisch müssen die Verantwortliche strategisch und die BetreiberIn operativ eine Mischstruktur etablieren, die die informationelle Gewaltenteilung – also die funktionale Differenzierung – innerhalb der Organisation durchsetzt. Technisch muss die BetreiberIn die Trennung so umsetzen, dass die Uploads nicht protokolliert werden können, weder auf

dem Server noch in ihrem Netzwerk. Die Verbindungen müssen zudem Ende-zu-Ende-verschlüsselt erfolgen und ggf. durch die Nutzung vorgeschalteter Anonymisierungsproxies (z.B. Tor) gesichert werden.

Ausblick

Mit unserer Intervention in die Debatte um den Einsatz von technischen Lösungen wie Tracing-Apps für gesellschaftliche Probleme in der Form einer Datenschutz-Folgenabschätzung haben wir eine öffentliche Debatte über die damit einhergehenden Risiken für Grundrechte und -freiheiten angestoßen und zugleich die notwendigen Informationen bereitgestellt, damit diese Debatte informiert geführt werden kann. Neben den beiden Aspekten, die wir in diesem Beitrag näher beleuchtet haben – der Unterscheidung zwischen Freiwilligkeit und Einwilligung sowie dem Problem von Personenbezug und Anonymisierung –, bietet die DSFA eine umfassende Analyse nicht nur der möglichen individuellen, sondern auch der gesellschaftlichen Auswirkungen, der rechtlichen, organisatorischen und technischen Anforderungen, die daher an solche Systeme zu stellen sind, sowie der erforderlichen Schutzmaßnahmen, mit denen die identifizierten Risiken so verringert werden können, dass die Anforderungen der DSGVO hinreichend erfüllt sind und ein verantwortbarer, beherrschbarer Betrieb des Verfahrens aufgenommen werden kann.

Mit der vorliegenden Datenschutz-Folgenabschätzung haben wir einen technischen, rechtlichen und methodischen Maßstab gesetzt, wie die Funktionen und die daraus sich ergebenden Datenschutzrisiken einer Tracing-App und des sie umgebenden Verfahrens für Betroffene in Zukunft zu analysieren, zu bestimmen und gegebenenfalls zu verringern sind.

Literatur

Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data. Working Paper 136.

Becker, Eberhard et al. (Hrsg.) (2003). Digital Rights Management: Technological, Economic, Legal and Political Aspects. Berlin: Springer Science & Business Media.

Bock, Kirsten et al. (2020). Datenschutz-Folgenabschätzung für die Corona-App. Version 1.6. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. URL: https://www.fiff.de/dsfa-corona.

Friedewald, Michael et al. (2016). Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz. White Paper, 1. Auflage, Forum Privatheit.

Podlech, Adalbert (1976). „Die Trennung von politischer, technischer und fachlicher Verantwortung in EDV-unterstützten Informationssystemen“. In: Informationsrecht und Informationspolitik. Hrsg. von Wilhelm Steinmüller. München: Oldenbourg Verlag, S. 207–216.

Pohle, Jörg (2018). Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung. Dissertation, Mathematisch-Naturwissenschaftliche Fakultät, Humboldt-Universität zu Berlin. URL: https://edoc.hu-berlin.de/handle/18452/19886.

Rost, Martin (2018). „Risiken im Datenschutz“. In: vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik, 57(1/2), S. 79–92.

1 Es handelt sich dabei um das Österreichische Rote Kreuz, das für seine „Stopp Corona“-App die DSFA Version 1.2 vom 22.04.2020 öffentlich bereitstellt. URL: https://www.roteskreuz.at/fileadmin/user_upload/Bericht_Datenschutzfolgeabschaetzung_StoppCorona_App.pdf (abgerufen am 27.04.2020).

2 URL: https://twitter.com/UlrichKelber/status/1247888280374235136 (abgerufen am 27.04.2020).

3 Die Verantwortung für die Entwicklung der App wurde nach öffentlicher Aussage der Bundesregierung inzwischen an T-Systems und SAP übertragen, wobei zugleich zum Zeitpunkt der Beitragsabfassung ein Vertrag noch nicht unterschrieben war.

4 Nach Angaben aus dem Digitalausschuss des Deutschen Bundestages plant die Bundesregierung nicht, eine gesetzliche Rechtsgrundlage zu schaffen, sondern setzt auf die informierte Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO.

Heinz Alenfelder

Videokonferenz-Software und der Datenschutz

Zur Zeit wird eine Unmenge von Artikeln über das Homeoffice in Tages- und Wochenzeitungen sowie online veröffentlicht. Darin taucht – allen Bedenken zum Trotz – immer wieder sowohl Teams von Microsoft als auch der durch viele Datenschutz-Lecks bekannte Dienst Zoom auf. Der Medienwissenschaftler Baumgärtel von der Hochschule Mainz stellte jüngst in der taz[1] fest: „Es kann nicht sein, dass als ein Ergebnis der Coronakrise nun proprietäre Programme wie Zoom oder Teams zum De-facto-Standard werden". Weiterhin hat das Fachmagazin IT-Sicherheit[2] im April über Phishing-Methoden berichtet, mit denen sich Cyberkriminelle den Hype um Videokonferenzen zu Nutze machen. Es beruft sich auf eine Analyse des amerikanischen Cybersecurity-Unternehmens Proofpoint, das erwartet, dass in Zukunft bekannte Markennamen wie Zoom und Cisco (Anbieter von WebEx) häufiger als Absender von Mails auftreten werden, die Malware verbreiten. Dennoch machen viele Arbeitgeber Vorgaben für Video- und Telefonkonferenzen. Aus unserer Sicht lautet verständlicherweise eine Kernfrage: Wie sieht die Situation aus dem Blickwinkel des Datenschutzes aus und was können Nutzerinnen und Nutzer tun?

Dieser Artikel stellt deshalb einige Leitfäden und Überblicke über Videokonferenz-Systeme von – teilweise als kritisch bekannten – Institutionen vor. Er zeigt darüber hinaus einige Fragen auf, die sich all diejenigen stellen sollten, die eine Videokonferenz-Software nutzen (müssen).

Informationen staatlicher Behörden

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** hat recht aktuell ein Kompendium Videokonferenzsysteme veröffentlicht[3]. Darin wird nach Beschreibung von Funktionsumfang, technischem Aufbau und Aspekten der Planung und des Betriebs von solchen Konferenzsystemen eine Gefährdungsanalyse vorgenommen. Exemplarisch werden dann drei Sicherheitskonzepte für verschiedene Beispielszenarien dargestellt, von denen vor allem das Szenario „Beispiel einer reinen Cloud-Lösung" eines Start-up-Unternehmens für die nicht-behördliche Praxis von Interesse sein könnte.

Auch der **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)** hat das Thema behandelt[4], kommt aber mit seinen Ausführungen deutlich knapper daher und nennt, wie das BSI, keine konkreten Anbieter. Jedoch zeigt er auf, welche Nebenbedingungen zu beachten sind und hat auch einige Leitfragen zur Beurteilung von Angeboten zusammengestellt[5].

Diverse **Landesdatenschutzbeauftragte** haben sich im April zu Wort gemeldet und Leitfäden veröffentlicht. So leitet der Baden-Württembergische LfDI beispielsweise seine Übersicht[6] mit den Worten ein: „Bei der Auswahl von Video- oder Telefonkonferenzsystemen sollte aus technischer Sicht darauf geachtet werden, dass der Anbieter weder Metadaten (wer hat wann mit wem kommuniziert) noch die Inhaltsdaten der Kommunikation für eigene Zwecke auswertet oder an Dritte weitergibt." Für konkrete Systeme gibt es Empfehlungen, die aber teils bereits kritisiert werden. Insbesondere die Grundeinstellung bei BigBlueButton, alle Sitzungen mitzuschneiden, stößt Informatikern böse auf[7]. Einzelfälle stellt der Ratgeber des LfDI selber kritisch klar, so etwa dass „die iOS-App Jitsi-Meet neben der Übertragung von Videosignalen auch Daten an den Hersteller und dessen Auftragsverarbeiter" überträgt. Schließlich verlinkt er auf Material aus Berlin. Die Berliner BfDI weist in einer Checkliste[8] explizit darauf hin, „dass einige verbreitet eingesetzte Anbieter die aufgeführten Bedingungen zu Redaktionsschluss (2. April 2020) nicht erfüllen, darunter Microsoft, Skype Communications und Zoom Video Communications". Das Schleswig-Holsteinische ULD schließlich unterscheidet in seinem Ratgeber[9] zwischen Hinweisen für Personen, die eine Videokonferenz organisieren und solchen, die daran teilnehmen. Für Erstere sind die Rahmenbedingungen zu klären; Letztere können vor allem durch Gestaltung ihres Umfelds und durch ihr Verhalten zur Datenschutzkonformität der Veranstaltung beitragen.

Eine komplette Auflistung oder gar die Analyse des einschlägigen Materials aller staatlichen Aufsichtsbehörden muss an dieser Stelle unterbleiben – nicht zuletzt, weil ständig neue Veröffentlichungen bzw. Aktualisierungen erfolgen.

Überblicke über Videokonferenz-Systeme

Vom Verein **Digitalcourage**, der die jetzt auf Herbst verschobenen Big-Brother-Awards federführend verleiht, werden drei Angebote hervorgehoben[10]: Jitsi Meet (das am besten in Googles Browser Chrome läuft), BigBlueButton (bei dem die Sicherheit vom Serverbetreiber abhängt, da auf dem Server nicht verschlüsselt wird) und Nextcloud Talk (das auf 4 Teilnehmende beschränkt ist und eine gemietete oder eingerichtete Nextcloud voraussetzt). Für reine Telefonkonferenzen wird Mumble empfohlen. Digitalcourage empfiehlt explizit nicht die Produkte Zoom, Skype (Microsoft), Discord und USA-basierte Dienste wie WebEx, GoToMeeting und LifeSize.

Der Informationsdienst **iRights.info** erwähnt in einem Artikel über Homeschooling[11] positiv die Angebote von Gotalk, Room sh und BlueJeans, verweist ansonsten aber auf Digitalcourage.

Auf der Webseite des **BfDI** in Bonn steht eine Auswahlhilfe des Niederländischen Datenschutzbeauftragten in deutscher Übersetzung zur Verfügung[12].

Auch bei der **Gesellschaft für Datenschutz und Datensicherheit (GDD)** findet sich eine Übersicht über die Großen der Branche. Die GDD hat die wesent-

lichen Eigenschaften von Konferenzanbietern im Anhang zur „Praxishilfe DSGVO XVI – Videokonferenzen und Datenschutz" zusammengefasst[13].

Heise.de schließlich bietet eine Liste von (kostenlosen) Videokonferenz-Tools an[14], weist dabei aber darauf hin, dass „lediglich TeamViewer Blizz eine Ende-zu-Ende-Verschlüsselung" nutzt, ohne das Heise das hätte überprüfen können. Die Empfehlung lautet hier, Jitsi auf einem eigenen Server zu installieren. In einer Meldung Ende April[15] verweist Heise.de auf einen Vergleich von 15 verschiedenen Videokonferenz-Lösung, den die Mozilla Foundation durchgeführt hat und in dem Verschlüsselung, Sicherheits-Updates, Passwort-Sicherheit, Schwachstellen-Umgang und Datenschutzrichtlinien verglichen wurden.

Fragen zur Nutzung von Videokonferenz-Systemen

Generell muss der Datenschutz bei Nutzung von Videokonferenz-Systemen aus verschiedenen Blickwinkeln betrachtet werden. Dabei geht es zunächst um die schlichte optische und akustische Verbindung zwischen den Teilnehmenden an der Konferenz. Weitergehende Problematiken wie Mitschnitte und deren Verwendung bis hin zur Veröffentlichung erfordern eine gesonderte Betrachtung, die hier nicht geleistet werden kann.

Einerseits können – vor allem im Rahmen von Homeoffice oder Homeschooling – in Videokonferenzen personenbezogene Daten im Gespräch oder per Übertragung des Bildschirm-Inhalts ausgetauscht werden. Wenn dies unumgänglich ist, ist dasselbe Verfahren anzuwenden wie bei der Datenverarbeitung im Betrieb oder in der Schule selbst. Die DSGVO gibt den Rahmen vor, betriebliche und staatliche Datenschutzbeauftragte geben Hilfestellung, zumeist – wie oben aufgeführt – in Form von Leitfäden oder bei konkreten Anfragen. Aus Hamburg wurde zwar über ein Verbot von Videokonferenzen durch die Aufsichtsbehörde berichtet, doch der Hamburgische Datenschutzbeauftragte stellte klar[16] „in enger Absprache mit der Behörde für Schule und Berufsbildung auf Überzeugungsarbeit bei den verantwortlichen Stellen, nicht aber auf Untersagungen und Verbote zu setzen".

Andererseits fallen eine Menge personenbezogener Daten über die einzelnen Beteiligten einer Videokonferenz beim Anbieter an, wie etwa Einwahl- und Teilnahme-Zeiten, IP-Adressen, Gerätedaten und die Gesprächsbeiträge samt Bilddaten aus dem heimischen Umfeld und vom Computer-Desktop. Deshalb sind bei der Auswahl eines Systems vielfältige Prüfungen zunächst der Rechtsgrundlagen und dann in Bezug auf mögliche Voreinstellungen, Profiling (Profilbildung der Nutzenden), Ende-zu-Ende-Verschlüsselung und Löschmöglichkeiten unabdingbar.

Im Zusammenhang mit einer Videokonferenz können die Beteiligten sich die folgenden Fragen stellen und beantworten.

Vor der Videokonferenz:

- Ist eine Videokonferenz das geeignete Mittel oder reicht auch eine Telefonkonferenz, ein Chat oder ein E-Mail-Wechsel?
- Von wo aus soll an der Videokonferenz teilgenommen werden? Ist die Datenübertragung im lokalen Netz/WLAN abgesichert?
- Speziell: Ist eine mobile Teilnahme, eventuell sogar im öffentlichen Raum, unbedingt notwendig? Wenn ja, übermittelt die App auch Daten an ihren Hersteller und könnte alternativ der Webbrowser genutzt werden?

Zur Vorbereitung der Videokonferenz:

- Sind alle Störelemente ausgeschaltet (bezogen auf Kamera-Aufnahmebereich, Mikrofon-Einstellungen, Datenübertragung von Bildschirminhalten, ausgeschaltete Sprachsteuerung des PCs und vorhandener Mobilgeräte)?
- Sind alle möglichen Einstellungen datenschutzfreundlich vorgenommen (Beispiele: Blurr-Effekt bei der Bildübertragung, Stummschaltung des Mikrofons in Redepausen, Ausschalten einer eventuellen Sprachanalyse für Untertitel und Transkribierung der Beiträge, Deaktivierung der Übermittlung von Absturzdaten)?
- Wurden Regeln für die Videokonferenz festgelegt und sind diese noch aktuell? Sollten Hinweise auf diese Regeln vor der Konferenz in Erinnerung gerufen werden (z. B. Verbot des Mitschnitts und einer Veröffentlichung)?

Während der Videokonferenz:

- Sind die Teilnehmenden alle bekannt, haben sie sich authentifiziert?
- Wird die Konferenz aufgezeichnet? Ist der Grund bekannt und triftig? Wurde dazu eine Einwilligung eingeholt?
- Signalisiert die Software die Kamera- und Mikrofon-Nutzung konkret? Gibt es eine Aufmerksamkeitsanzeige, die die aktive Teilnahme an der Konferenz überwacht? Ist diese unumgänglich?
- Muss im Einzelfall der Bildschirminhalt unbedingt geteilt werden oder reicht auch eine mündliche Erklärung des zu zeigenden Dokuments?

Nach der Videokonferenz:

- Ist die Konferenz auch wirklich beendet, d. h. wurde der Prozess seitens des Betriebssystems aus dem Speicher entfernt?
- Kann die Kamera- und Mikrofon-Nutzungserlaubnis für das Konferenz-System zurückgenommen werden?
- Ist eine Aufzeichnung der Konferenz verfügbar, wo liegt diese und wann wird diese gelöscht?
- Sind Metadaten vorhanden und können sie gelöscht werden?

Diese Liste von Fragen erhebt keinerlei Anspruch auf Vollständigkeit, sondern sie versucht, über die Krisenzeit hinaus für einen bewussteren Umgang mit Videokonferenz-Systemen und deren Nutzung zu sensibilisieren.

Alle Webseiten wurden am 2. Mai 2020 zuletzt besucht.

1 „Digital unabhängig werden" Debattenbeitrag in der taz, 23.04.2020, S. 12

2 https://www.itsicherheit-online.com/blog/detail/sCategory/222/blogArticle/4284

3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.html;jsessionid=30D457459CF2B0A34528AF8E11AE2FF6.2_cid341

4 https://www.bfdi.bund.de/DE/Datenschutz/Datenschutz-Corona/Kommunikation/Inhalt/Messenger_Videokonferenzdienste.html?cms_templateQueryString=videokonferenz&cms_sortOrder=score+desc

5 https://www.bfdi.bund.de/DE/Datenschutz/Datenschutz-Corona/Kommunikation/Inhalt/Beurteilung_Angebote_Messenger.html?nn=13881424

6 https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/

7 https://twitter.com/beatdoebeli/status/1254686918857678848

8 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Checkliste_Videokonferenzen.pdf

9 https://www.datenschutzzentrum.de/uploads/it/ULD-Ploetzlich-Videokonferenzen.pdf

10 https://digitalcourage.de/blog/2020/corona-homeoffice-tipps

11 https://irights.info/artikel/unterricht-zu-hause-und-was-macht-der-datenschutz/30017

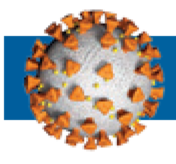
12 https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Auswahlhilfe-Messenger-Systeme.pdf?__blob=publicationFile&v=1

13 https://www.gdd.de/downloads/praxishilfen/ph_videokonferenzsysteme_aktuelle-tabelle/view

14 https://www.heise.de/ct/artikel/Kostenlose-Videokonferenz-Programme-im-Funktionsueberblick-4704912.html

15 https://www.heise.de/newsticker/meldung/Mozilla-veroeffentlicht-Report-zu-Videokonferenzdiensten-4710756.html

16 https://datenschutz-hamburg.de/pressemitteilungen/2020/03/2020-03-26-falschmeldung-skype



Corona-Nachrichten

Bund

RKI präsentiert „Datenspende-App“

Das Robert-Koch-Institut (RKI) präsentierte am 07.04.2020 eine App mit dem Namen „Corona-Datenspende“, um im Kampf gegen das Coronavirus (SARS-CoV-2 bzw. Covid-19) Daten von Fitnessbändern und Smartwatches zu sammeln, über die ergänzende Informationen erlangt werden sollen, wo und wie schnell sich das Coronavirus ausbreitet. Die App ist für iOS und Android-Geräte verfügbar; die Nutzung ist freiwillig. Das RKI sammelt die Daten auf pseudonymer Basis und sagt zu, keine Stammdaten der Nutzenden wie Namen und Anschrift zu sammeln. Es behauptet, es könne einzelne Nutzende nicht identifizieren.

- Die App

Die Corona-Datenspende-App dient nicht der Nachverfolgung von Kontaktpersonen, sondern soll – ergänzend zu weiteren Datenquellen, z.B. den offiziellen Meldedaten – dabei helfen, Infektionsschwerpunkte besser zu erkennen und dazu beitragen, ein genaueres Bild über die Wirksamkeit der Maßnahmen zur Bekämpfung von Covid-19 zu gewinnen. Die Idee der App beruht darauf, dass viele Menschen in Deutschland regelmäßig mit Smartwatches oder Fitnessarmbändern ihre Vitaldaten aufzeichnen. Demgemäß werden Aktivitäts- und Schlafdaten, Pulsschlag und Körpertemperatur erfasst und ausgewertet, sofern dies vom jeweiligen Modell des Geräts unterstützt wird. Bei einer akuten Atemwegserkrankung ändern sich diese Vitalzeichen in den meisten Fällen deutlich. Daher könnten auch typische COVID-19-Symptome wie Fieber durch die App erkannt werden.

Mit Hilfe der Corona-Datenspende-App stellt der Nutzer des Mobilgeräts diese Daten dem RKI zur Verfügung. Zur Lokalisierung des Nutzers soll dieser zusätzlich seine Postleitzahl eingeben. Die Corona-Datenspende-App fragt zudem einmalig Körperdaten ab zu Geschlecht, Alter, Größe und Gewicht. Die Daten werden in groben Schritten (+/- 5 kg bzw. 5 cm) erfasst. Die Daten werden wissenschaftlich aufbereitet und fließen im Anschluss in eine Karte ein. Diese zeigt die regionale Verbreitung potenziell Infizierter bis auf Ebene der Postleitzahl. Die Karte wird regelmäßig aktualisiert und unter www.corona-datenspende.de veröffentlicht.

Prof. Lothar H. Wieler, der Präsident des RKI, warb für die App: „Wenn in einer ausreichend großen Stichprobe die Anzahl der symptomatischen Patienten erfasst werden kann, könnte uns das dabei helfen, früher Rückschlüsse auf Infektionsgeschehen, Verbreitung und auch auf die Wirksamkeit der bisherigen Maßnahmen zu ziehen. Die App erkennt Symptome, kann aber keine Erkrankung nachweisen. Sie ersetzt keine offiziellen Meldezahlen und keinen Labortest auf das Coronavirus, ist aber eine wichtige Ergänzung.“ In den USA hätten sich ähnliche Fallschätzungen auf Basis von Smartwatch- und Fitnessarmband-Daten in Grippewellen als sehr treffgenau erwiesen.

Das RKI teilte mit, es habe die App gemeinsam mit dem e-Health-Unternehmen Thryve und unter Einbeziehung des Bundesdatenschutzbeauftragten (BfDI) entwickelt. Dem RKI geht es dabei nicht darum, COVID-19 im Einzelfall zuverlässig zu diagnostizieren und die Tests auf das Virus zu ersetzen. Ebenso wenig ersetzt sie den öffentlichen Meldeweg zur Erfassung der Infektionszahlen. Mit den Daten sollen vielmehr die Maßnahmen zur Eindämmung von COVID-19 sinnvoll ergänzt werden, so Wieler: „Wir wünschen uns, dass sich viele Menschen beteiligen. Denn je mehr Menschen ihre Daten für eine Auswertung zur Verfügung stellen, desto genauer werden unsere Erkenntnisse zur Verbreitung des Coronavirus.“

Auf die Kritik von Datenschutzseite hin bestätigte das RKI, dass jedem Nutzer eine individuelle Nutzer-ID zu-

geordnet wird: „Nur so können Daten auch über längere Zeiträume richtig zugeordnet und interpretiert werden." Die mit Dienstleistern getroffenen Vereinbarungen über die Datenverarbeitung würden „den Anforderungen des Art. 28 DSGVO genügen".

Das RKI wirbt unter dem Slogan „Hände waschen, Abstand halten, Daten spenden." Innerhalb der ersten 24 Stunden wurden auf der Webseite 50.000 Downloads verzeichnet. Nach einer Woche hatten mehr als 300.000 Menschen die App heruntergeladen und installiert.

Die Datenspende-App des RKI erhielt im Nachhinein einen wissenschaftlichen Segen durch die „Dritte Ad-hoc-Stellungnahme Coronavirus-Pandemie – Die Krise nachhaltig überwinden" der Nationalen Akademie der Wissenschaften Leopoldina vom 13.04.2020:

Traditionelle epidemiologische Melde- und Monitoringsysteme, die systembedingt nur mit erheblicher Zeitverzögerung und lückenhaft Daten liefern, sollten durch innovative Methoden aus der digitalen Epidemiologie ergänzt werden. Ansätze zur „digitalen Datenspende" bieten eine innovative Technologie. Zum Beispiel können bundesweite Umfragen per Smartphone-App Daten des aktuellen Gesundheitszustands der Bevölkerung liefern. Zudem könnten Apps zur freiwilligen Mitteilung von Symptomen und Informationen zum eigenen Krankheitsverlauf nützliche Daten liefern. Fitness-Tracker und sog. Wearables zeichnen Daten zum Ruhepuls und zu Schlafrhythmen auf, deren Analyse das Auftreten von Fieber und grippeähnlichen Symptomen anzeigen kann. Dringend erforderlich ist hier die weitere Erforschung und Überprüfung der Zuverlässigkeit und Validität dieser Daten. Die digitalen Datenspenden müssen in partizipatorische Projekte eingebettet sein, in denen Bürgerinnen und Bürger zum Allgemeinwohl und gemeinschaftlich zur Eindämmung der Pandemie beitragen können. Dabei sollten sie anonymisiert, sicher und geschützt ihre Daten als Fundament für bessere Prognosen zur Verfügung stellen können. Ein verantwortungsvoller Umgang - unter Gewährleistung eines verlässlichen Schutzes der Privatheit - mit diesen Daten und deren Qualitätssicherung kann durch Datentreuhänder sichergestellt werden. Datenspenden sollten durch breite Medienkampagnen begleitet werden, die ihren gemeinnützigen Charakter vermitteln. Schon existierende oder in der Entwicklung befindliche Projekte dieser Art in der eHealth-Startup-Szene sollten identifiziert und koordiniert werden.

In den nächsten Wochen und Monaten sollte die Zahl der Neuinfektionen soweit wie möglich kontrolliert auf einem niedrigen Niveau gehalten werden. Dabei sind Kurzzeitprognose-Modelle immer mit aktualisierten, hochaufgelösten Daten anzupassen. Ziel ist es, die wahrscheinliche Entwicklung der Pandemie über 1 bis 2 Wochen (inkl. anzugebender Ungenauigkeitsintervalle) vorherzusagen und die erwartete Effektivität von Maßnahmen vor deren Anwendung zu vergleichen. Auch der Effekt einer Lockerung von Maßnahmen kann in verschiedenen Szenarien untersucht werden. Die Modellvorhersagen bieten insbesondere auch ein Instrumentarium, um objektivierbare Kriterien für einen schrittweisen Übergang in den Normalzustand auf der Grundlage des verfügbaren Wissens zu entwickeln. Ziel ist es, die zu erwartenden wiederkehrenden regionalen Cluster, in denen Infektionen zeitlich und räumlich gehäuft auftreten, frühestmöglich zu erkennen und durch passgenaue regionale Maßnahmen aufzulösen. In Regionen mit niedrigen Infektionsraten und geringem Verbreitungspotential könnten einschränkende Maßnahmen, ggf. auch spezifisch für einzelne Personengruppen, gelockert werden. Nicht zuletzt sollte die erwartete Wirkung eines gezielten Einsatzes der ermittelten immunen Personen in kritischen Bereichen (Pflege, Altenheime, Krankenhäuser) durch die Modellvorhersagen erfasst werden. Ebenso müssen indirekte Effekte auf gefährdete Bevölkerungsgruppen Berücksichtigung finden.

- Umstrittene Finanziers

Die allgemeinen Geschäftsbedingungen der App offenbaren, dass das deutsche Unternehmen, das die App umsetzt, ein hochbewertetes Berliner StartUp ist. Ein Firmenportrait der mHealth Pioneers GmbH legt die Hintergründe des 2017 gegründeten Unternehmens offen. Danach gehört zu den bekanntesten deutschen Investoren Carsten Maschmeyer, der zuletzt in der TV-Produktion Höhle des Löwen quasi am Fließband nach neuen Unternehmensideen und Geschäftskonzepten suchte. Maschmeyer ist umstritten; die Berichterstattung rund um den von ihm mitgegründeten Finanzdienstleister AWD, dessen Verkaufsmethoden über Jahre in der Kritik standen, zog rechtliche Auseinandersetzungen nach sich. Zu den weiteren Investoren zählt Min-Sung Sean Kim, der für Samsung in die Bereiche künstliche Intelligenz und Gesundheitsdaten investiert.

- Kritik von Datenschützern

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Ulrich Kelber, relativierte seine Unterstützung: „Ich erwarte zusätzlich, dass regelmäßig evaluiert wird, ob die App ihren Zweck erfüllt. Tut sie das nicht, muss die Verarbeitung beendet werden." Der Name der App sei irreführend, da man bei Teilnahme an der Erhebung das Recht an den Daten nicht abgebe. Nutzer könnten „ihre Einwilligung jederzeit widerrufen". Außerdem müsse das Institut noch konkretisieren, wie lange Informationen gespeichert würden. Das RKI habe zugesagt, dass in diesem Fall alle gesammelten Daten gelöscht werden. Das Datenschutzniveau sei bei Fitness-Trackern und Smartwatches je nach Hersteller sehr unterschiedlich. Diese Schnittstelle sei aus seiner Sicht „wahrscheinlich das größte Problem".

Die Gesellschaft für Informatik (GI) hält die App „Corona-Datenspende" für unausgegoren, wenn nicht kontraproduktiv. Die Anwendung erfülle „im Hinblick auf Datenschutz und IT-Sicherheit nicht die grundlegenden Anforderungen". Das RKI habe damit eine Chance vertan, das Vertrauen in digitale Anwendungen zur Eindämmung des Coronavirus zu stärken. Die GI ist zwar überzeugt, dass digitale Instrumente potenziell hilfreich sind, um Neuinfektionen zu verringern und nachzuverfolgen. Sie mahnt aber: „Dabei sollten sie jedoch dem Stand der Forschung und den höchsten Anforderungen in Sachen Transparenz, Zweckgebundenheit, Wahrung der Privatsphäre, Anonymisie-

rung, Prüfbarkeit, Verschlüsselung und Datensparsamkeit entsprechen." Die GI kritisiert, „dass der Code der Anwendung proprietär ist, und damit nicht öffentlich dokumentiert und überprüfbar, wie eigentlich für solche Apps zwingend notwendig". Auch weitere wichtige Prinzipien wie Zweckgebundenheit, Anonymität, Datensparsamkeit und Schutz vor unbefugten Zugriff seien „entweder nicht erfüllt oder zumindest unklar".

GI-Präsident Hannes Federrath verweist auf das Anfang April vorgestellte PEPP-PT-Rahmenwerk zur Kontaktverfolgung: „Es gibt sehr gute Ansätze, mit digitalen Werkzeugen der Verbreitung des Virus entgegenzuwirken." Leider sei die vorliegende Datenspende-Anwendung dagegen „überraschend schlecht gemacht und daher dem Schutz der Bevölkerung eher abträglich". Der Informatikprofessor hofft, dass das RKI „als wichtige Vertrauensinstanz in der aktuellen Krise" bei künftigen digitalen Instrumenten wie der geplanten Tracking-App mehr Sorgfalt walten lasse.

Der EU-Abgeordnete Patrick Breyer stellte dem RKI am 08.04.2020 in einem offenen Brief elf Fragen zu der App. Das Mitglied der Piratenpartei wundert sich etwa, warum die Anwendung nicht als Open-Source-Lösung verfügbar gemacht werde, warum die Datenschutz-Folgeabschätzung nicht öffentlich sei und wieso keine schnellstmögliche Anonymisierung der überlassenen Informationen erfolge. Der Parlamentarier beklagte: „Dass eine Regierungsbehörde medizinische Daten zehn Jahre lang personenbeziehbar speichern will, stellt eine völlig neue Gefährdung der Privatsphäre dar."

Am 20.04.2020 veröffentlichte der Chaos Computer Club (CCC) eine Schwachstellenanalyse der App in Form eines Blackbox-Tests. Der Quellcode der App wurde nicht offen gelegt. Gemäß dem CCC werden die Gesundheitsdaten bei Nutzern von Google Fit, Fitbit, Withings sowie Polar – nicht von Apple Health – direkt vom Server des jeweiligen Fitnessarmband-Herstellers an das RKI übertragen, statt zunächst an das Smartphone des Nutzers und sodann von dort an das RKI gesendet zu werden. Bei einer Übertragung via Smartphone könnte durch die App auf dem Smartphone sichergestellt werden, dass wirklich nur diejenigen Daten an das RKI übertragen werden, die auch gespendet werden sollen, und dass sie zudem vor der Übertragung pseudonymisiert würden. So hingegen erhält das RKI Zugriff auf den Account des jeweiligen Nutzers auf dem Server des Fitnessarmband-Herstellers und kann von dort theoretisch sämtliche Nutzerdaten abrufen, also beispielsweise auch Gesundheitsdaten aus dem Zeitraum vor der Corona-Krise oder den vollständigen Namen des Nutzers. In der Datenschutzerklärung heißt es dagegen fälschlich: „Erfasste Daten werden von meinem Smartphone verschlüsselt zu den von uns ausschließlich in Deutschland betriebenen Servern übertragen, dort verarbeitet und gespeichert. Die App hat zu keinem Zeitpunkt Zugriff auf unmittelbar identifizierende Informationen wie Namen oder Adresse." Das RKI pseudonymisiert die Daten erst, nachdem sie auf seinem Server angekommen sind. Damit besteht auch die Gefahr, dass etwaige Angreifer, denen es gelingt, die Server des RKI zu kompromittieren, auf die Accounts der Datenspender bei den Herstellern ihrer jeweiligen Fitnessarmbänder zugreifen können.

- Kommentar aus der DANA-Redaktion

Es ist richtig, dass die Epidemiologen und die Politik möglichst zeitnah möglichst valide Daten über die Gesundheitssituation der Bevölkerung benötigen, um kurzfristig adäquate Maßnahmen, also notwendige, wirksame und verhältnismäßige Maßnahmen ergreifen zu können. Doch ist die Idee des RKI, das über sog. Datenspenden von Fitnesstrackern und Smartwatches zu verwirklichen, die mit Medienkampagnen beworben werden, keine gute Idee: Dies läuft auf eine Werbemaßnahme für derzeit existierende Gesundheitstracker hinaus, bei denen der Datenschutz zumeist nicht im Ansatz gewährleistet ist; die Validität der erhobenen Daten ist teilweise sehr schlecht. Apple und Google als Plattform- und Betriebssystemanbieter von iOS und Android erhalten dabei regelmäßig Gesundheitsdaten frei Haus geliefert, darüber hinaus viele weitere in die Apps eingebundene „befreundete Unternehmen". Anonym sind diese Daten für diese Unternehmen nicht, aber nicht einmal für das RKI, von der Leopoldina als „Datentreuhänder" bezeichnet. Diese Daten sind allenfalls pseudonym, d.h. jederzeit einer Person wieder zuordnenbar. Beim RKI unterliegen diese Daten keiner strengen Zweckbindung; das RKI unterliegt als Forschungseinrichtung insofern nicht der beruflichen Schweigepflicht, wie man sie bei behandelnden oder beratenden Ärzten oder auch Rechtsanwälten oder Pfarrern kennt. Die Polizei könnte sich mit einem entsprechenden Beschluss also Zugriff auf die gesammelten Daten verschaffen und sie beispielsweise zur Kriminalitätsbekämpfung verwenden. Ein Forschungsgeheimnis, von Forschern und Datenschützern seit Jahren gefordert, hat die Politik bisher nicht für nötig gehalten, wäre aber heute dringender denn je, um Menschen Vertrauen und rechtliche Sicherheit zu geben.

Quellen: Robert Koch-Institut, PM v. 07.04.2020, Mit Daten von Fitnessarmbändern und Smartwatches mehr über die Verbreitung des Coronavirus erfahren; Lücking, Dein Herz schlägt für Maschmeyer, www.neues-deutschland.de 07.04.2020; Krempl, Corona: Informatiker kritisieren „Datenspende-App" als „schlecht gemacht", www.heise.de 10.04.2020, Kurzlink: https://heise.de/-4701353; Leistner, Risiken und Nebenwirkungen: Wie sicher ist die Corona-Datenspende-App für Nutzer? www.euronews.com 08.04.2020; Leopoldina, Corona-Pandemie – Die Krise nachhaltig überwinden, 13.04.2020, S. 6; van Lijnden, Corona-App verstößt angeblich gegen eigene Datenschutzerklärung, www.faz.net 20.04.2020; Kuketz, CCC deckt auf: Datenspende-App des RKI mit schweren Mängeln www.kuketz-blog.de 20.04.2020).

Bundesweit

Drohnentests zur Corona-überwachung

Während Drohnen, die Corona-Ausgangsbeschränkungen kontrollieren und zum Zuhausebleiben aufrufen, im Ausland mancherorts schon gängige Praxis sind, ist der Einsatz von Drohnen zur Kontrolle im Kampf gegen das Coronavirus in Deutschland bislang noch eher die Ausnahme.

Eine Sprecherin des Landesamts für Zentrale Polizeiliche Dienste Nordrhein-Westfalen bestätigte, dass zehn Polizeibehörden in Düsseldorf und Dortmund den Einsatz von jeweils zwei Drohnen testen, zuletzt auch im Zuge der Coronakrise. Die kleinen Flugobjekte würden unter anderem eingesetzt, um Orte abzusuchen und Menschen an beliebten Sammelpunkten per Lautsprecher vor den gesundheitlichen Risiken allzu großer Nähe zu warnen. Letzteres sei vergleichbar mit Durchsagen eines Streifenwagens. Ein Sprecher der Düsseldorfer Polizei betonte, dass die Kamera der Drohne nicht zur Identifizierung Einzelner diene: „Es werden auch keine Bilder gespeichert." Es gehe nur um Übersichtsaufnahmen, vor allem bei schwer zu überblickenden Gebieten. Die Reaktionen der Menschen seien „durchaus positiv". Viele zeigten sich auch an der Technik interessiert.

Die hessische Polizei verfügt über zehn Drohnen unterschiedlicher Größen. Gemäß dem Innenministerium waren diese am 02.04.2020 in Frankfurt zur Überwachung der Corona-Kontaktregeln im Einsatz, als es darum ging, ob in Parks womöglich illegale Abiturfeiern stattfinden. In Mecklenburg-Vorpommern nutzte die Feuerwehr im April eine Drohne, um einzelne Strände auf der Insel Rügen zu kontrollieren. Das Gerät kann mit seiner Wärmebildkamera auch Grillpartys erkennen.

Die beiden großen Polizeigewerkschaften halten Drohnen für ein mögliches Instrument, um Ausgangsbeschränkungen zu überwachen. Für die Deutsche Polizeigewerkschaft (DPolG) erklärte deren Vorsitzender Rainer Wendt, man würde den Einsatz der Flugobjekte „sehr begrüßen: Zur unterstützenden Nutzung durch die Einsatzkräfte wäre der Einsatz von Drohnen hilfreich und wünschenswert. Deshalb sind die Ministerien gut beraten, diese Kapazitäten bereitzustellen und auszubauen." Auch aus Sicht der Gewerkschaft der Polizei (GdP) können Drohnen in bestimmten Situationen sinnvoll sein, so der stellvertretende Bundesvorsitzende Jörg Radek: „Wir müssen aber sensibel sein. Drohnen sind ein neues Einsatzmittel und könnten bei vielen Bürgern den Eindruck erwecken, wir seien auf dem Weg in den Überwachungsstaat."

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit, Ulrich Kelber, erklärte: „Grundsätzlich gelten für den Einsatz von Drohnen die gleichen datenschutzrechtlichen Regeln wie für die Videoüberwachung." Die Polizei dürfe Drohnen nur zweckgebunden einsetzen, um konkrete Aufgaben zu erfüllen: „Das schließt einen anlasslosen und flächendeckenden Einsatz aus."

In vielen Bundesländern setzt die Polizei bisher auf herkömmlichere Methoden, um Corona-Regelverstöße zu ahnden und aufzuklären. Eine Sprecherin der niedersächsischen Polizei erklärte, man weise über Durchsagen mit Lautsprecherwagen auf rechtliche Vorgaben hin. Für die Zukunft schließt sie einen Corona-bedingten Einsatz von Drohnen aber nicht aus: „Die aktuelle Beschränkung sozialer Kontakte zur Eindämmung der Verbreitung der Corona-Pandemie könnte perspektivisch eine solche Lage darstellen." Bayern verzichtet absehbar auf Corona-Kontroll-Drohnen. Auch in Baden-Württemberg, Hamburg und Brandenburg erklärten die Behörden, die kleinen Flugkörper nicht zur Überwachung zu nutzen. In Sachsen-Anhalt wurde die Einhaltung der Corona-Beschränkungen an den Ostertagen aus der Luft per Hubschrauber überwacht, so ein Ministeriumssprecher: „Damit können wir vor allem in den späten Abendstunden überwachen, ob partiell Osterfeuer abgebrannt werden, da diese aus der Luft besser erkennbar sind." Drohneneinsätze waren nicht geplant (Wagner, Drohnen gegen „Corona"-Verstöße? www.e110.de 16.04.2020).

Bundesweit

Aldi Süd kontrolliert Marktzugang digital

Der Discounter Aldi Süd will in der Corona-Krise mit digitalen Zutrittskontrollen die Zahl der Kunden in seinen Filialen begrenzen. Sensoren an den Ein- und Ausgängen sollen dabei die Kundenzahl im Laden in Echtzeit überwachen. Aldi-Manager Malte Kuhn erklärte am 27.04.2020: „Das Zugangssystem gewährleistet, dass die Auslastungshöchstgrenzen in unseren Filialen nicht überschritten werden." Insgesamt will der Discounter die Hälfte seiner 1930 Filialen mit den Sensoren ausstatten. Die Filialmitarbeiter werden dabei automatisch über eine App, per SMS oder Anrufe über die Auslastung informiert. In einzelnen Filialen soll ein Ampelsystem oder eine Bildschirmanzeige getestet werden, die die Kunden über die Auslastung der Filiale informiert und so den Zugang steuert (Aldi Süd setzt wegen Corona auf digitale Zutrittskontrollen, rp-online.de 27.04.2020).

Hessen

Corona-Bekämpfung mit Palantir

Hessens Covid-19-Krisenstab nutzt künftig Software des US-Unternehmens Palantir, um den Überblick über die Corona-Krise zu behalten. Das zum Einsatz kommende Programm heißt „Foundry". Es handelt sich um eine so genannte Datamining-Software, die wie andere Programme von Palantir Daten aus verschiedenen Quellen zusammenführt, um Verbindungen zwischen Informationen zu ziehen, die Menschen in kurzer Zeit nicht erkennen könnten. Mit dem Programm soll gemäß einem Sprecher des hessischen Innenministeriums die Covid-19-Pandemie praktisch in Echtzeit dargestellt werden: „Der Landeskrisenstab plant die Nutzung einer Software der Firma Palantir, um allgemein zugängliche Informationen, wie die Verteilung von Infektionen mit dem Coronavirus, Bettenkapazitäten oder die Versorgung mit Schutzausstattung in einem umfassenden Lagebild darzustellen." Die aktuelle Situation solle schnell bewertet werden und „Hilfe und Material dort ankommen, wo sie am dringendsten benötigt werden. Wenn beispielsweise die Infektionszahlen in einem Kreis mit erhöhter Altersstruktur und bereits hoher Auslastung der stationären Einrichtungen stark ansteigen, kann so frühzeitig die Entscheidung getroffen werden, vorgeplante Versorgungseinrichtungen zu aktivieren und die erforderliche Schutzausstattung bereitzustellen."

Die Software greife nicht auf „individualisierte Person- oder Patientendaten" zu. Ihr Einsatz sei mit dem hessischen Datenschutzbeauftragten abgestimmt.

In einer Stellungnahme erklärte Palantir, die Daten in Foundry seien gut geschützt, durch „granulare Zugriffskontrollen, Anonymisierung, sichere Speicherung und Löschung sowie umfassende Auditierungs- und Aufsichtsfunktionen". Palantir bot auch der Bundesregierung seine Software an. Das Bundesgesundheitsministerium arbeitet aber nicht mit dem Unternehmen zusammen.

Palantir wurde anfangs mit Geld aus dem Investment-Arm der CIA finanziert. Zu den besten Kunden des Unternehmens aus Kalifornien gehört der amerikanische Militär- und Geheimdienstkomplex. Dessen Analysten durchforsten mit Software der Firma die großen Datenmengen, die sie jeden Tag zusammensammeln. Deshalb sehen Datenschützer und Oppositionspolitiker den Einsatz von Software des Unternehmens kritisch, auch wegen der Historie US-amerikanischer Spionage in Deutschland. Mitgegründet wurde Palantir vom Facebook-Investor und ehemaligen Trump-Berater Peter Thiel.

Das Unternehmen dient sich Behörden weltweit oft unentgeltlich im Kampf gegen Covid-19 an. Gemäß Hessischem Innenministerium wird die Software „dem Krisenstab zunächst kostenfrei und befristet zur Verfügung gestellt." Das Frankfurter Polizeipräsidium nutzte als erste Polizeibehörde bereits die Palantir-Software „Gotham". Damit können u.a. Informationen aus Polizeidatenbanken für Kriminalfälle und Fahndungen, Verbindungsdaten aus der Telefonüberwachung, und Informationen aus dem Facebook-Profil von Verdächtigen verknüpft werden. Nach Beginn des Pilotprojektes stellte die Opposition im hessischen Landtag die Frage, ob die heiklen Daten der deutschen Polizei wirklich vor dem Zugang der US-Regierung sicher seien, wenn Techniker von Palantir die Technik im Polizeipräsidium aufsetzten. Sie hielt auch die Vergabe des Auftrags, dessen Preis geheim gehalten wurde, für so intransparent, dass sich ein Untersuchungsausschuss mit den Kontakten der Landesregierung zu Palantir befasste. Der grüne Bundestagsabgeordnete Konstantin von Notz kritisierte die aktuellen Pläne aus Hessen: „Dass das Innenministerium auch nach einer intensiven öffentlichen Debatte und in dem Wissen, dass es zahlreiche Alternativen gibt, an der hochumstrittenen Firma Palantir als Zulieferer festhält, ist äußerst bedauerlich." Solche Entscheidungen zerstörten das Vertrauen der Bürger. „Für die Verantwortlichen vor Ort kann man nur hoffen, dass sich das nicht irgendwann böse rächt" (Brühl, Hessens Krisenstab erntet Kritik für Einsatz von Palantir-Software, www.sueddeutsche.de 21.04.2020).

Nachtrag: Kurz vor Redaktionsschluss dieser DANA entschied sich die hessische Landesregierung, bei der Corona-Bekämpfung auf den Einsatz der Palantir-Software entgegen ursprünglicher Absichten zu verzichten.

Niedersachsen

Gesundheitsämter übermitteln Coronalisten an Polizei

Niedersachsens Gesundheitsämter übermitteln Daten von Coronavirus-Infizierten an die Polizei und setzen sich damit über die Kritik der Landesbeauftragten für den Datenschutz (LfD) Barbara Thiel hinweg. Auch Namen und Adressen von Menschen, die mit ihnen Kontakt hatten, stehen auf den sogenannten Quarantänelisten. Mit Erlass vom 31.01.2020 wurden die Gesundheitsämter der Landkreise und kreisfreien Städte durch das Gesundheits- und Sozialministerium auf Veranlassung des Innenministeriums zur Weitergabe der Daten in einem Schreiben veranlasst. Thiel forderte daraufhin am 03.04.2020 die Behörden auf, ihre Anordnung umgehend zurückzunehmen. Ein Sprecher des Innenministeriums reagierte: „Natürlich nehmen wir die Kritik der Landesdatenschutzbeauftragten sehr ernst und werden die aufgeworfenen Fragestellungen nochmals prüfen." Kurz darauf wurde die Anordnung durch einen neuen Erlass bestätigt.

Der Datenschutzblog Freiheitsfoo veröffentlichte einen kurzen Ausschnitt aus dem neuen Erlass. Demnach bezieht sich das Innenministerium nicht mehr nur auf das Niedersächsische Polizei und Ordnungsbehördengesetz (DANA 3/2019, 155) und das Infektionsschutzgesetz des Bundes, sondern argumentiert auch mit dem sogenannten rechtfertigenden Notstand aus dem Strafgesetzbuch (§ 34 StGB). Was genau darüber hinaus noch in dem Erlass steht, blieb zunächst unbekannt: Selbst die Mitglieder des Innenausschusses des Landtags erhielten ihn zunächst nicht. Er regele „interne Abläufe und ist nicht für eine Weitergabe bestimmt".

Thiel reagierte umgehend: „Diese Rechtsauffassung teile ich ausdrücklich nicht. Selbstverständlich handelt es sich bei den übermittelten Daten um sensitive Gesundheitsdaten. Zwar werden die Daten auf der Grundlage des Infektionsschutzgesetzes mit dem Ziel verarbeitet, die Verbreitung übertragbarer Krankheiten zu verhindern. Eine fachspezifische Übermittlungsbefugnis an die Polizeileitstellen umfasst das Infektionsschutzgesetz jedoch nicht." Auch die Voraussetzungen des rechtfertigenden Notstands seien nicht für sämtliche Personen gegeben, deren Daten pauschal an die Polizei übermittelt werden.

Thiel kann die Weitergabe der Listen nicht selbst stoppen: Den Landesgesetzen zufolge kann sie zwar Anordnungen erteilen, diese aber nicht vollstrecken (DANA 2/2019, 79; 4/2018, 200 f.). Oppositionspolitiker fordern deshalb, sie mit weitergehenden Rechten auszustatten, so etwa Marco Genthe, innenpolitischer Sprecher der FDP-Fraktion im Landtag: „Sonst muss man sich ehrlicherweise irgendwann mal fragen, wozu wir eine Landesdatenschutzbeauftragte haben". Er hält die Übermittlung der Daten für verfassungswidrig. Die innenpolitische Sprecherin der Grünen-Fraktion Susanne Menge forderte, die Weitergabe der Daten auszusetzen, bis eine Lösung gefunden ist, gemeinsam mit Thiel. Sie wirft der rot-schwarzen Landesregierung vor, Entscheidungen wie diese vorbei am Parlament zu treffen. „Auch in einer Krisenzeit kann man nicht plötzlich autokratische Strukturen durchsetzen."

Menge hat Anfang April beim Innen- sowie beim Sozialausschuss eine Unterrichtung über die Rechtsgrundlage der Coronavirus-Listen beantragt – sowohl durch die Landesregierung, als auch durch die Landesdatenschutzbeauftragte.

Uta Schöneberg, Leiterin des Rechtsreferats des Landespolizeipräsidiums begründete den Erlass: „Die Polizei benötigt diese Daten ausschließlich zu Zwecken der Eigensicherung." Auf

Nachfrage räumte sie aber ein, die niedersächsische Polizei würde auch Strafverfahren einleiten, wenn mithilfe der übermittelten Daten Quarantäneverstöße deutlich würden. Die Daten würden ausschließlich durch die Leitstellen der Polizei aufbewahrt und nicht in die polizeilichen Systeme eingepflegt. Diese Maßgabe galt aber erst nach der Erneuerung des Erlasses. Die Ereignisse hätten sich „ein bisschen überschlagen. Für die Polizeidirektionen war aber klar – wir hatten schon die ganze Woche vorher das Thema – dass die Daten nicht in die Systeme eingepflegt werden dürfen."

Den Zahlen des Robert Koch-Instituts zufolge waren Anfang April in Niedersachsen insgesamt 6.385 Menschen an Covid-19 erkrankt. Die Namen vieler von ihnen sowie von deren Angehörigen dürften bei der Polizei gelandet sein. Der Leiter des Corona-Krisenstabs, Staatssekretär im Sozialministerium Heiger Scholz (SPD) erklärte, die Quarantänelisten ließen nicht darauf schließen, wer tatsächlich krank ist und wer nicht: „Dass wir hier hochsensible Gesundheitsdaten weitergeben, das bestreite ich."

Dem widersprach Thiel: „Selbstverständlich handelt es sich bei den übermittelten Daten um sensitive Gesundheitsdaten. Offenbar hat auch das Ministerium selbst erkannt, dass es sich unbestreitbar um Gesundheitsdaten handelt. Immerhin ist in dem neuen Erlass die Rede von ‚Patienten'."

Thilo Weichert, Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz, bezeichnete Scholz' Argumentation als „absoluten Schwachsinn". Er rät allen Menschen, die in Niedersachsen derzeit unter Quarantäne stehen, möglichst bald Strafanzeige gegen das Sozialministerium zu stellen. Seiner Einschätzung nach verstößt die Weitergabe der Daten gegen die ärztliche Schweigepflicht. Bei Verstößen droht eine Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe. In Niedersachsen könnten sie tausendfach begangen worden sein (Laufer, Niedersachsen schickt weiter Coronalisten an die Polizei, www.netzpolitik.org 08.04.2020; Die Landesbeauftragte für den Datenschutz Niedersachsen, PE 07.04.2020, Landesdatenschutzbeauftragte fordert erneut sofortigen Übermittlungsstopp von Corona-Gesundheitsdaten an die Polizei).

Mecklenburg-Vorpommern

Infiziertendaten für Polizei mit dem Segen des „Datenschutzes"

Das Gesundheitsministerium des Landes Mecklenburg-Vorpommern bestätigte, dass es in einem Schreiben an Landkreise und kreisfreie Städte diese aufgefordert habe täglich bis 10.00 Uhr Listen mit namentlicher Nennung der Covid-19-Infizierten an die beiden Polizeipräsidien weiterzugeben. Dies wertet der Linke-Landtagsabgeordnete Peter Ritter als einen Verstoß gegen den Datenschutz und die ärztliche Schweigepflicht: „Es besteht die Gefahr, dass dem Missbrauch personenbezogener Daten Tür und Tor geöffnet wird." In einem nächsten Schritt gebe es dann vielleicht eine Mitteilung an Supermärkte, welche Kunden das Virus haben.

Nach Meinung des Landesdatenschutzbeauftragten Heinz Müller indes liegt der Vorgabe ein berechtigtes Interesse der Polizei zugrunde, die bei Einsätzen etwa gegen häusliche Gewalt wissen müsse, ob ein Infektionsrisiko für sie bestehe: „Die Abwägung gegenüber den Interessen von Erkrankten ist zugegebener Maßen schwierig. Aber, wenn wir das Infektionsrisiko verringern können, sollten wir es tun." Doch müsse mit den personenbezogenen Daten äußerst sorgsam umgegangen werden, mahnte der Datenschützer. Ritter dagegen hält die regelmäßige Datenübermittlung zu Infizierten für unzulässig: „Meine Fraktion erwartet, dass derlei Meldepraxis und Stigmatisierung von möglicherweise infizierten Personen unterbleibt."

Nicht nur aus Mecklenburg-Vorpommern und Niedersachsen (s.o.) gibt es Nachrichten über unzulässige Datenübermittlungen von Gesundheitsämtern an die Polizei. In Baden-Württemberg haben mit Unterstützung des Innenministers Thomas Strobl mehrere Gesundheitsämter Daten von Corona-Infizierten weitergegeben – weil sich die Polizei vor Infektionen schützen müsse. Der Landesbeauftragte Stefan Brink kritisierte, dass diese Daten rechtswidrig übermittelt wurden und forderte ihre Löschung. In Bremen musste die dortige Datenschutzbeauftragte Imke Sommer eine vergleichbare Praxis stoppen (Sauer, Covid-19-Infizierte in MV werden an Polizei gemeldet, www.nordkurier.de 30.03.2020; Polizei im Angriff auf Grundrechte (1), extradienst.net 03.04.2020).

Saarland

Temperaturkontrolle an Edeka-Eingang

In Saarbrücken scannte „Edeka Lonsdorfer" von allen Kundinnen und Kunden die Körpertemperatur mit einer Wärmebildkamera in Echtzeit am Eingang der Filiale in der Mainzer Straße. Die Behörde der saarländischen Landesbeauftragten für Datenschutz hat deshalb ein Verwaltungsverfahren eröffnet. Ein Mitarbeiter sprach die Passierenden bei erhöhter Temperatur an. Gab es hierfür keine Erklärung, musste der Kunde den Laden verlassen.

Marco Schömer von der saarländischen Datenschutzbehörde erklärte, das System widerspreche der Datenschutzgrundverordnung (DSGVO). Das Recht auf informationelle Selbstbestimmung der Kunden werde verletzt. Sie könnten klagen, weil die Kamera gegen die Persönlichkeitsrechte geht. Der Geschäftsführer von „MATEC Sicherheitssysteme", der Saarbrücker Firma, die das Sicherheitssystem eingebaut hat, erklärte, Kunden und Mitarbeiter würden sich sicherer fühlen. Das Vorgehen sei mit einem Anwalt abgesprochen gewesen: Die Wärmebildkamera sei DSGVO-konform, weil sie die Daten nicht speichere.

Dem entgegnet Schömer: „Wenn jemand – ob krank oder kerngesund – von den Augen anderer Kunden zur Rede gestellt wird, besteht ganz klar die Gefahr der Stigmatisierung." Auf der Facebook-Seite von „MATEC Sicherheitssysteme" wird für die Thermalkamera mit dem Einsatz im Großmarkt von „Schwamm" in der Bismarckstraße in Saarbrücken geworben. Hier wird die Kamera zum Fieber-Screening von Mitarbeitern genutzt. Laut „Schwamm" befindet sich die Kamera am Personaleingang. Fremde Menschen würden nicht erfasst (Wegen Corona: Supermarkt scannt Kunden am Eingang - Datenschutz-Experte entsetzt, www.focus.de 16.04.2020).

Schleswig-Holstein

UKSH plant Corona-Biobank

Das Universitätsklinikum Schleswig-Holstein (UKSH) will eine Corona-Biobank aufbauen. Sie soll in das von der Bundesregierung ins Leben gerufene Covid-19-Forschungsnetz der Universitätsmedizin eingebettet werden. Joachim Thiery, Vorstand für Forschung und Lehre am UKSH, begründete das Projekt: „Wir vermuten, dass Covid-19 nicht nur zu fürchterlichen Akutschäden, sondern auch zu Folgeerkrankungen führt“. Möglichst alle Schleswig-Holsteiner, die eine Corona-Infektion überstanden haben, sollen dafür über einen Zeitraum von mindestens zehn Jahren gründlich nachuntersucht werden sowie Blutproben abgeben. Hintergrund seien „Berichte beispielsweise zu neurologischen Störungen“ infolge des Virus. Befürchtet würden Herzinfarkte oder Schlaganfälle noch Jahre nach einer überstandenen Covid-19-Infektion. „Die überschießende Entzündung verursacht bei manchen Patienten schwere Schädigungen der inneren Aderhaut, die Mikrogerinnsel auslösen könnten.“ Auch Blutdruckregulation und Leber seien betroffen.

Das UKSH hat jahrzehntelange Erfahrungen mit seiner Biobank „popgen“, die chronische Krankheiten auf Populationsebene abbilde. Thiery erklärt, dass sich Schleswig-Holstein besonders für solche hochstandardisierten Sammlungen eignet, „da wir mit Dänemark im Norden, den Meeren im Westen und Osten natürliche Barrieren bei der Krankenversorgung und wenig Abwanderung von Patienten haben“. Das Projekt werde in enger Kooperation mit allen deutschen Universitätskliniken laufen – koordiniert von der Berliner Charité. Zur noch nicht gesicherten Finanzierung erläutert Thiery: „Verglichen mit den unübersehbaren Kosten von Corona-Folgeerkrankungen – möglicherweise in Milliardenhöhe, wenn wir zu spät kommen – liegt unser Projekt im Bereich weniger Millionen pro Jahr“ (Uniklinik Schleswig-Holstein will Corona-Biobank aufbauen, www.oldenburger-onlinezeitung.de 17.04.2020; „Schädigung des Herzens“, Der Spiegel Nr. 17 v. 18.04.2020, 18).

Weltweit

Amazon checkt Körpertemperatur von Mitarbeitern

Der Online-Versandhändler Amazon setzt an einigen Standorten Wärmebildkameras zur Eindämmung des Coronavirus ein. Um die Gesundheit und Sicherheit der Mitarbeiter zu unterstützen, werde bereits täglich ihre Temperatur gemessen, erklärte Amazon-Sprecherin Kristen Kish auf Anfrage. An einigen Standorten würden nun zusätzlich Wärmebildkameras eingesetzt, an welchen, gab sie nicht bekannt. Amazon wird vorgeworfen, in der Corona-Krise nicht genug für den Schutz der Mitarbeiter zu unternehmen. Der Konzern hatte deshalb schon mit Protesten und Arbeitsniederlegungen zu kämpfen (Amazon nutzt Wärmebildkameras, SZ 20.04.2020, 18).

Weltweit

Facebook beschafft Forschern COVID-19-Symptomdaten

Gemäß einer Ankündigung durch Facebooks Gründer und Chef Mark Zuckerberg am 20.04.2020 fordert das Online-Netzwerk Facebook seine mehr als 2,5 Milliarden Nutzenden weltweit auf, an einer Umfrage der Universität von Maryland zur Verbreitung von Coronavirus-Symptomen teilzunehmen. Die zunächst auf die USA beschränkte Aktion solle nun global durchgeführt werden. Facebook als Plattform mit Milliarden Mitgliedern sei in einer einzigartigen Position, um Wissenschaftlern und Behörden zu helfen.

Die Forschenden der Universität Carnegie Mellon veröffentlichten am selben Tag erste Erkenntnisse aus der seit Anfang April laufenden Umfrage in den USA. Demnach bekommen sie pro Woche Antworten von rund einer Million Facebook-Nutzenden. Daraus lasse sich zum Beispiel ableiten, dass in einigen New Yorker Vororten zwei bis drei Prozent der Einwohner Covid-19-Symptome hätten. Die weltweite Umfrage wird von der Universität von Maryland organisiert. Facebook soll keinen Zugang zu den Antworten der Nutzenden haben.

Facebook macht zudem aggregierte Daten öffentlich, die Aufschluss über die Mobilitätsströme inmitten von Ausgeh- und Kontaktbeschränkungen geben. Ähnliche Informationen gibt es auch zum Beispiel von Mobilfunk-Anbietern sowie Apple und Google (Facebook will Link zu Corona-Umfrage weltweit anzeigen, www.frankenpost.de 20.04.2020; Fragen an Milliarden, SZ 21.04.2020, 16).

Auszug aus der „Bayerischen Staatszeitung“ Nr. 14 v. 03.04.2020, S. 2

Die Frage der Woche: Sollen zur Eindämmung des Coronavirus Handydaten genutzt werden dürfen?



Bild: iStock

Ja

Alfred Winter, Präsident der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS)

Handys mit Bluetooth sind geeignet, um Kontakte von Infizierten mit nicht infizierten Personen im Nachhinein zu ermitteln. Wenn zwei teilnehmende Handys nahe beieinander sind, kann eine App Kontaktinformationen austauschen. Die Privatsphäre aller Beteiligten wird dabei gewahrt, weil keine persönlichen Informationen ausgetauscht werden müssen. Es müssen auch keine Informationen über Ort und Zeitpunkt des Kontakts in zentralen Datenbanken gespeichert werden. Mit der Einrichtung einer neutralen Treuhandstelle können die identifizierenden Daten von Personen strikt von den Kontaktinformationen getrennt werden.

Dazu müssen sich die Personen, welche die App nutzen möchten, bei der Treuhandstelle registrieren lassen. Um sich zu registrieren, gibt zum Beispiel Frau Müller ihre E-Mail-Adresse bei der Treuhandstelle ab und bekommt eine zufällig erzeugte Nummer zurück, das Pseudonym. Die Treuhandstelle merkt sich nur, welche E-Mail-Adresse zu welchem Pseudonym gehört. Kommt nun das Handy von Frau Müller nahe am Handy von Herrn Meier vorbei, werden lediglich die Pseudonyme der beiden ausgetauscht. Die Pseudonyme werden nur eine begrenzte Zeit gespeichert, vielleicht 18 Tage. Sollte Herr Meier kurze Zeit später positiv auf das Coronavirus getestet werden, übermittelt er mit seiner App alle noch gespeicherten Pseudonyme an die Treuhandstelle, die dann Frau Müller und andere Personen, die in letzter Zeit in der Nähe von Herrn Meier waren, informieren kann. Bei solchen Verfahren hält die GMDS Kontaktermittlungs-Apps für sehr sinnvoll und auch vertretbar.

Wie in vielen Bereichen der medizinischen Forschung ist auch hier die Aufklärung und die Einwilligung der Nutzer erforderlich, auch um unnötige Verängstigungen zu vermeiden. So kann moderne Technologie eine Epidemie eindämmen helfen, ohne die Privatsphäre zu verletzen. Das massenhafte Auslesen von Verbindungsdaten in sogenannten Funkzellen ist dagegen viel zu ungenau und schafft riesige Datenschutzprobleme.

Nein

Frank Spaeing, Vorsitzender der Deutschen Vereinigung für Datenschutz e.V. (DVD)

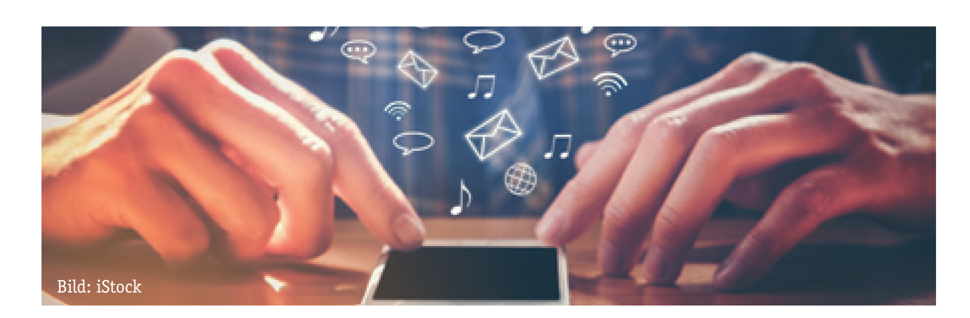
Frau Merkel sagt, dass wir das Corona-Virus besiegen können, ohne unsere freiheitlichen und demokratischen Prinzipien aufgeben zu müssen. Daran sollten sich alle orientieren, die angesichts des Rückgangs der Infektionszahlen im Polizeistaat China meinen, einer derartigen Gesundheitsherausforderung könne man nur mit autoritären Mitteln Herr werden. Das Gegenteil ist richtig: Die wirksamsten Mittel gegen eine Pandemie sind solche, die von den Menschen verstanden und freiwillig mitgetragen werden. Aktuell gibt es eine große Bereitschaft der Bürger, sich bewusst einzuschränken. Ob dies ausreicht, muss immer wieder neu geprüft werden; wenn nicht, kann und darf der Gesetzgeber rigider vorgehen; geeignet, erforderlich und verhältnismäßig muss es dennoch sein.

Digitale Technik kann einen Beitrag leisten, um Betroffenen zusätzlichen Schutz zu geben. Ob die Mobilfunkdaten der Telekom hilfreich sein werden, kann man bezweifeln. Sind diese, wie angegeben, aggregiert und damit anonym, haben wir kein Datenschutzproblem. Apps auf Mobilgeräten mit einer präzisen Lokalisierungsfunktion, etwa mit GPS, könnten die Nutzenden informieren, wann und wo sie sich in einem Risikogebiet aufhalten. Mit Bluetooth-Lösungen könnte gar eine Warnung von Gerät zu Gerät bei räumlicher Nähe ohne zentrale Datenzusammenführung erfolgen.

Wer wirksam die Quarantäne von Angesteckten zu Hause überwachen will, der kann sich mit Smartphone-Tracking nicht begnügen. Das kann man zu Hause lassen, wenn man sich – illegal außer Haus – mit Freunden trifft. Nötig wäre dann eine elektronische Fußfessel, die wir bisher nur für terroristische Gefährder und schwere Straftäter kennen. Südkorea hat gezeigt, dass man mit intensivem Testen die Ansteckungsraten stark senken kann. Eine medizinische Lösung der Corona-Krise bekommt unserer Demokratie mehr als eine polizeistaatliche. Zumal rechte politische Kräfte an einer solchen Lösung Gefallen finden würden – auch für die Zeit nach der Krise.

Digitale Gesellschaft / Digitalcourage / Deutsche Vereinigung für Datenschutz / Netzwerk Datenschutzexpertise – Pressemitteilung vom 4.3.2020

Europäische Menschenrechts- und Digitalrechtsorganisationen warnen vor illegalen Online-Werbemethoden durch Apps


Bild: iStock

- Digitalcourage, Digitale Gesellschaft, Deutsche Vereinigung für Datenschutz und das Netzwerk Datenschutzexpertise fordern Datenschutzbehörden auf, Datenweitergabe bei Apps wie z. B. Grindr, Tinder und OkCupid zu untersuchen (Text der Aufforderung unten)
- Studie „Out of Control“ belegt Weitergabe sensibler Daten wie Standort, sexuelle Orientierung, religiöse und politische Überzeugungen

Auf Einladung der Civil Liberties Union for Europe haben zehn Menschenrechts- und Digitalrechtsorganisationen in sieben EU-Ländern die Datenschutzbehörden in ihren Ländern aufgefordert, Verstöße gegen die europäische Datenschutz-Grundverordnung (DSGVO) durch Smartphone-Apps wie z. B. Grindr, Tinder und OkCupid zu untersuchen. **In Deutschland appellieren die Digitale Gesellschaft, Digitalcourage, die Deutsche Vereinigung für Datenschutz und das Netzwerk Datenschutzexpertise an die Datenschutzaufsichtsbehörden**, auf der Grundlage einer umfassenden Analyse [1] mit dem Titel **„Out of Control“** (Außer Kontrolle) gegen App-Betreiber vorzugehen, die ohne wirksame Einwilligung der Nutzenden hochsensible Daten erheben und für Werbezwecke nutzen. An der Kampagne sind weitere Nicht-Regierungsorganisationen aus Kroatien, Italien, Ungarn, Slowenien, Spanien und Schweden beteiligt. Die Analyse wurde vom Norwegischen Verbraucherrat (Norwegian Consumer Council – NCC) und der österreichischen Organisation für digitale Rechte noyb [2] durchgeführt.

Die in der Analyse untersuchten Mobil-Apps, darunter **Dating- und Menstruationszyklus-Apps**, leiten die sensiblen Informationen ihrer Nutzerinnen und Nutzer über deren genauen **Standort, sexuelle Orientierung, religiöse und politische Überzeugungen und viele weitere persönliche Informationen** an zahlreiche Drittfirmen in einem intransparenten Werbetechnologie-Ökosystem weiter. So verteilt die weltweit verbreitete Dating-App Grindr [3] die Nutzungsdaten, etwa auch die aktuellen Lokalisierungsangaben, an mehr als ein Dutzend weiterer Unternehmen. Die Dating-App OkCupid listet über 300 Werbe- und Analyse-„Partner“.

Friedemann Ebelt von **Digitalcourage**: *„Smartphone-Nutzer haben regelmäßig keine Chance, sich vor den Folgen der Datenausbeutung und der massiven kommerziellen Überwachung zu schützen. Diese Folgen können für den Einzelnen gravierend sein bis hin zu einer Gefährdung von Leib und Leben. Die hochsensitiven Persönlichkeitsprofile haben das Potenzial, die privaten Freiheiten in unserer Gesellschaft zu untergraben“.*

Elke Steven von der **Digitalen Gesellschaft**: *„Die Daten der App-Nutzenden werden unter Verletzung der Regeln der Datenschutz-Grundverordnung verarbeitet. Die eingeholten Zustimmungen zur Auswertung sind absolut intransparent und verstoßen zudem gegen nationales und europäisches Verbraucherrecht.“*

Frank Spaeing, Vorsitzender der **Deutschen Vereinigung für Datenschutz**: *„Die europäischen Datenschutzbehörden müssen dringend schneller und effektiver zusammenarbeiten, um den täglich millionenfach stattfindenden Rechtsbruch zu ahnden und zu beenden. Dafür müssen sie besser als bisher ausgestattet werden.“*

Thilo Weichert vom **Netzwerk Datenschutzexpertise**: *„Der augenblickliche Zustand ist nur schwer zu ertragen: Kleinere Verstöße werden derzeit schon wirksam verfolgt. Doch bei den oft dramatischen Verletzungen des Datenschutzes durch internationale Internet-Unternehmen muss sich die Wirksamkeit der DSGVO erst noch erweisen. In dieser Auseinandersetzung gegen die Daten-Goliaths benötigen die Aufsichtsbehörden die Unterstützung der Öffentlichkeit, der Verbraucherschützer und der Politik.“*

Weitere Informationen finden Sie auf der Webseite der Kampagne #StopSpyingOnUs [4].

Detaillierte Informationen zum Real Time Bidding, welches in der Analyse „Out of Control“ eine Rolle spielt, können Sie dem DANA-Sonderheft 3-2019 entnehmen: https://www.datenschutzverein.de/wp-content/uploads/2019/09/DANA_19_3_Sonderheft_Real_Time_Bidding.pdf

Für weitere Einzelheiten über die Kampagne wenden Sie sich bitte an:

Friedemann Ebelt,
friedemann.ebelt@digitalcourage.de
Frank Spaeing,
spaeing@datenschutzverein.de
Elke Steven,
elke.steven@digitalegesellschaft.de
Thilo Weichert,
weichert@netzwerk-datenschutzexpertise.de

Für Fragen zu den Organisationen in den anderen europäischen Staaten wenden Sie sich an Orsolya Reich,
o.reich@liberties.eu

[1] Siehe https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

[2] Siehe https://noyb.eu/out-of-control/?lang=de

[3] Grindr bezeichnet sich selbst als das weltgrößte soziale Netzwerk für schwule, queere, bi- und transsexuelle Menschen, mit der sich Menschen in der näheren Umgebung lokalisieren und kontaktieren können. Siehe https://www.grindr.com/

[4] Siehe https://www.liberties.eu/de/campaigns/stopspyingonus-fixad-tech-kampagne/307

Schreiben an die deutschen Datenschutzaufsichtsbehörden

Die Industrie für digitale Werbung verletzt die Privatsphäre der Verbraucher

Sehr geehrte Damen und Herren,

wir möchten Ihre Aufmerksamkeit auf einen am 14. Januar 2020 vom norwegischen Verbraucherrat (Norwegian Consumer Control) veröffentlichten Bericht [1] lenken, der sich mit den verborgenen Seiten der Datenwirtschaft auseinandersetzt. Der Bericht mit dem Titel „Out of Control" („Außer Kontrolle") beschreibt, wie das Online-Marketing in der Werbebranche (Adtech) funktioniert. Er kommt dabei zu dem Schluss, dass das umfassende Nachverfolgen (Tracking) und das Erstellen von individuellen Profilen (Profiling), die das Herzstück des derzeitigen Adtech-Ökosystems bilden, von Grund auf missbräuchliche Praktiken sind, die gegen die Europäische Datenschutz-Grundverordnung (DSGVO) verstoßen.

Die Menschen tragen ihre Mobiltelefone überall mit sich herum und die Geräte zeichnen Informationen über sensible Themen wie Gesundheit, Verhalten, Interessen und sexuelle Orientierung auf. Der Bericht konzentriert sich auf die persönlichen Daten, die von mobilen Anwendungen gesammelt werden, und auf das dahinter verborgene informationstechnische Ökosystem. Er wirft ein Licht auf die kommerziellen Dritten, die im Hintergrund bleiben und heimlich, still und leise unsere persönlichen Daten erhalten und auswerten. Die Analyse in dem Bericht umfasst 10 Apps aus verschiedenen Kategorien (z.B. Dating, Fruchtbarkeits-Tracking, Kinder-Apps) und identifiziert die wesentlichen Probleme:

Persönliche Daten werden systematisch abgesaugt und von diversen Unternehmen unter fragwürdigem und falschem Verweis auf nicht anwendbare Rechtsgrundlagen und in jedem Fall ohne Wissen oder Kontrolle der Verbraucherinnen und Verbraucher verwertet. Insbesondere gilt dabei:

Die Unternehmen erhalten **keine wirksame Einwilligung** der Verbraucherinnen und Verbraucher zur Verarbeitung ihrer persönlichen Daten, auch nicht für die Verarbeitung von Daten, die unter Artikel 9 (besondere Datenkategorien) der DSGVO fallen und daher eine ausdrückliche Zustimmung erfordern.

Die **Unternehmen erfüllen auch nicht die Voraussetzungen, um berechtigte Interessen als Rechtsgrundlage** für die Datenverarbeitung (gemäß Art. 6 Abs. 1 lit. f DSGVO) anführen zu können. Diese Regelung würde ohnehin keine geeignete Rechtsgrundlage für die im Bericht analysierten Verarbeitungsvorgänge darstellen. Die umfassende Profilierung und Kategorisierung von Verbraucherinnen und Verbrauchern dient nicht nur der gezielten Werbung, sondern ist auch noch in verschiedenen anderen Bereichen schädlich und zwar sowohl für die einzelnen Bürgerinnen und Bürger als auch für die Gesellschaft als Ganzes. Zu den negativen Auswirkungen gehören verschiedene Formen der Diskriminierung und der Exklusion, weit verbreiteter Betrug, Manipulation und nicht zuletzt die abschreckende Wirkung, die **massive kommerzielle Überwachungssysteme** sowohl auf Einzelpersonen als auch ganz allgemein auf demokratische Debatten haben können.

Die **einzelnen Personen können dem Tracking nicht ausweichen**, erstens, weil sie nicht mit den notwendigen Informationen versorgt werden, um beim ersten Start der Apps eine informierte Entscheidung zu treffen, zweitens aber auch, weil ihnen als Betroffenen das Ausmaß der Verfolgung, des Datenaustauschs und der allgemeinen Komplexität des Adtech-Ökosystems unverständlich bleibt. Der Einzelne kann nicht wirklich entscheiden, wie seine persönlichen Daten gesammelt, geteilt und verwendet werden.

Selbst wenn einzelne Bürgerinnen und Bürger umfassende Kenntnisse über die Funktionsweise der Adtech-Technologie hätten, gäbe es immer noch nur sehr begrenzte Möglichkeiten, die Datenausbeutung zu stoppen oder zu kontrollieren. Die Anzahl und Komplexität der Akteure, die am Adtech-Ökosystem beteiligt sind, ist erschütternd. Den einzelnen Personen steht so keine sinnvolle Möglichkeit zur Verfügung, sich zu wehren oder sich anderweitig zu schützen.

Aus all dem folgt, dass die im gesamten Adtech-Ökosystem stattfindende massive kommerzielle Überwachung in einem systematischen Widerspruch zu den notwendigen Rahmenbedingungen der Demokratie steht. Studien haben gezeigt, dass Individuen ihr Verhalten entsprechend verändern, wenn sie das Gefühl haben, dass ihre Handlungen erfasst werden und möglicherweise gegen sie verwendet werden können. **Im System des Ad-Tracking wird im Grunde alles aufgezeichnet und für nicht vorhersehbare Zwecke nutzbar gemacht.** Dies kann Folgen auf die Art und Weise haben, wie wir das Internet nutzen und darauf, ob wir bereit sind, nach bestimmten Informationen über die Arbeitsweise unserer Institutionen oder über das Handeln der Politik zu suchen. Und das ist auch der Grund, warum die kommerzielle Überwachung langfristig schwerwiegende Folgen für den Zugang der Menschen zu Informationen, für ihre Meinungsfreiheit, für die demokratischen Institutionen und für die Gesellschaft als Ganzes haben kann.

Eine massive kommerzielle Überwachung kann unsere Grundrechte und Freiheiten auch auf direktere Weise gefährden. In Ägypten zum Beispiel hat die Polizei die Dating-App Grindr eingesetzt, um Homosexuelle zu identifizieren und zu verhaften [2]. Wenn Standortdaten an Hunderte von Unternehmen weitergegeben werden, muss nur eines dieser Unternehmen die Daten selbst weitergeben oder gehackt werden, um Menschen in physische Gefahr zu bringen.

Auf Grundlage dieser Erkenntnisse hat der norwegische Verbraucherrat bei der norwegischen Datenschutzbehörde eine Reihe von Beschwerden gegen verschiedene Adtech-Firmen und die Dating-App Grindr eingereicht. Die nationalen Regulierungs- und Aufsichtsbehörden müssen aktive Maßnahmen ergreifen, um diese Probleme anzugehen und um durchzusetzen, dass die Adtech-Industrie ihre Arbeitsweise grundlegend ändert.

Wir hoffen, dass Sie unsere Bedenken bezüglich der in diesem Bericht angesprochenen Themen teilen. Die Untersuchung wurde in Norwegen durchgeführt, aber einige der analysierten Anwendungen (z.B. Grindr, siehe https://de.wikipedia.org/wiki/Grindr und dort Entstehung und Verbreitung, oder auch Tinder, siehe https://tinder.com/?lang=de) sind auch in Deutschland tätig, und die Adtech-Firmen, gegen die sich die Beschwerde des norwegischen Verbraucherrats wie auch von noyb [3] richtet, verarbeiten mit hoher Wahrscheinlichkeit auch Daten deutscher Verbraucherinnen und Verbraucher.

Wir bitten Sie daher dringend, diesen dargestellten Problemen nachzugehen und die norwegische Aufsichtsbehörde bei der Bearbeitung der Originalbeschwerden durch parallele Bemühungen innerhalb der EU zu unterstützen. Die Bedenken, die durch die kommerzielle Überwachung und die Praktiken der Adtech-Industrie aufgeworfen werden, betreffen die gesamte EU.

Über eine Rückmeldung zu Ihren geplanten Aktivitäten zu diesen Problemen möchten wir Sie bitten.

Dieses Schreiben ist in enger Zusammenarbeit der Deutschen Vereinigung für Datenschutz mit Digitalcourage, der Digitalen Gesellschaft, dem Netzwerk Datenschutzexpertise und Liberties.eu entstanden.

Als Anlage zu diesem Schreiben haben wir Ihnen das DANA-Sonderheft 2-2019 mit dem Themenschwerpunkt Real Time Bidding beigefügt [4]; in diesem werden einige Themen besprochen, die auch im Bericht angesprochen werden.

[1] Siehe https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

[2] Siehe z.B. Article 19: LGBTQ ONLINE Summary Report. Apps, arrests and abuse in Egypt, Lebanon and Iran. February 2018. https://www.article19.org/wp-content/uploads/2018/02/LGBTQ-Apps-Arrest-and-Abuse-report_22.2.18.pdf

[3] Siehe https://noyb.eu/out-of-control/?lang=de

[4] https://www.datenschutzverein.de/wp-content/uploads/2019/09/DANA_19_3_Sonderheft_Real_Time_Bidding.pdf

Pressemitteilung der Gesellschaft für Freiheitsrechte (GFF) vom 27.12.2019

Studie: Handyauswertung bei Geflüchteten ist teuer, unzuverlässig und gefährlich

Das Bundesamt für Migration und Flüchtlinge (BAMF) analysiert routinemäßig die Mobiltelefone asylsuchender Menschen. Die Datenträgerauswertung ist kostspielig, intransparent, generiert kaum verwertbare Ergebnisse und verletzt Grundrechte, so das Ergebnis einer heute von der Gesellschaft für Freiheitsrechte e.V. (GFF) veröffentlichten Studie.

Die Studie „Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa [2]“ befasst sich mit der im Jahr 2017 eingeführten Analyse elektronischer Datenträger durch das BAMF. Wenn eine asylsuchende Person weder Pass noch Passersatzdokument vorweisen kann, ist die Behörde dazu berechtigt, ihr Smartphone auszuwerten, um Hinweise auf Identität und Herkunft zu erhalten. Analysiert werden Kontakte, ein- und ausgehende Anrufe und Nachrichten, Browserverläufe, Geodaten aus Fotos sowie verwendete Emailadressen und Benutzernamen auf Plattformen wie Facebook, booking.com und Tinder. Ein konkreter Verdacht, dass die asylsuchende Person

über ihre Identität oder ihr Herkunftsland lügt, ist nicht erforderlich.

„Handys enthalten unzählige persönliche Daten. Ein staatlicher Zugriff darauf ist deshalb an hohe verfassungsrechtliche Hürden geknüpft. Indem das BAMF ohne konkrete Verdachtsmomente die Handys geflüchteter Menschen durchleuchtet, missachtet es diese Vorgaben eklatant“, sagt Lea Beckmann, Juristin bei der GFF und Co-Autorin des Berichts. „Es verletzt damit das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme von zigtausenden Menschen – und das für wenig aussagekräftige Ergebnisse.“

Seit der Einführung des Verfahrens im Jahr 2017 hat das BAMF hochgerechnet etwa 20.000 Mobiltelefone von Asylsuchenden ausgelesen und über 11 Millionen Euro in dieses Verfahren investiert. Im Zeitraum Januar 2018 bis Juni 2019 scheiterte das Auslesen in etwa einem Viertel der Fälle bereits an technischen Problemen. Mehr als die Hälfte der erfolgten Datenträgerauswertungen erwiesen sich als unbrauchbar. Nur in 1-2% der verwertbaren Auswertungen fanden sich Widersprüche zu den Angaben, die die Asylsuchenden selbst in ihren Befragungen gemacht hatten. Von der Einführung des Handydatenauslesen profitierten also in erster Linie die Technologiehersteller.

„Die Auswertung von Handydaten durch das BAMF zeigt die Grenzen unseres Rechtsschutzsystems: Die Betroffenen haben praktisch keine Möglichkeit, sich dagegen zu wehren. Nur das Bundesverfassungsgericht kann das zugrundeliegende Gesetz für verfassungswidrig erklären und kippen. Ein solches Gerichtsverfahren ist langwierig und kostspielig. Für die einzelne Person kommt Hilfe dann längst zu spät“, kritisiert Beckmann. „Wir wollen helfen, diese Rechtsschutzlücke zu schließen. Deshalb bereiten wir derzeit gemeinsam mit betroffenen Personen und engagierten Kooperationsanwälten rechtliche Schritte gegen die Datenträgerauswertung vor.“

Für die Studie werteten die Journalistin Anna Biselli und die Juristin Lea Beckmann einen umfangreichen Quellenbestand aus, darunter Ergebnisberichte von Datenträgerauswertungen, Asylakten, interne Dienstanweisungen, Handbücher und Schulungsunterlagen des BAMF, Dokumente aus dem Gesetzgebungsverfahren, Stellungnahmen von Rechtswissenschaftler*innen, Flüchtlingsorganisationen und Verbänden, sowie Informationen, die durch parlamentarische Anfragen in Bundestag und Landesparlamenten öffentlich wurden. Zudem führten die Autorinnen Hintergrundgespräche mit Geflüchteten, Anwält*innen und Rechtswissenschaftler*innen, Verfahrensberatungsstellen und Menschenrechtsorganisationen in Deutschland und anderen Ländern Europas.

Die Studie „Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa“ finden Sie unter: https://freiheitsrechte.org/studie-handydatenauswertung

Presserklärung des Gen-ethischen Netzwerks und des Netzwerks Datenschutzexpertise vom 06.02.2020

Gefährlicher Unsinn bei mymuesli: genetische Konsumberatung

Das Gen-ethische Netzwerk und das Netzwerk Datenschutzexpertise warnen Verbraucher*innen vor dem aktuellen Angebot von mymuesli. Unter dem Namen „myDNA slim“ bietet das Unternehmen für 189 Euro einen DNA-Test zur Ernährungsoptimierung an.

Mit den „lebenswichtigen“ Informationen sollen Kund*innen ihre „ganz persönliche Verstoffwechselung von den sogenannten Makronährstoffen (Kohlenhydrate, Fette und Proteine)“ erfahren. Verharmlosend ist von einem „Ernährungstest“ die Rede: „Du möchtest Dich in Deinem Körper fit und wohl fühlen? Unser DNA-Test kann Dir dabei helfen.“

Isabelle Bartram, Molekularbiologin vom Gen-ethischen Netzwerk: „Hier werden auf einer unseriösen Basis hochsensitive Daten erfasst, ohne dass das Unternehmen auf die Nebenfolgen hinweist. Mymuesli macht auf Öko, Bio und Nachhaltigkeit. Tatsächlich werden hier unter dem Anschein von Wissenschaftlichkeit falsche gesundheitliche Versprechen gemacht – das belegen auch die von mymuesli selbst zitierten Studien. DNA-Personalisierung im Konsument*innenbereich ist aus fachlicher Sicht nicht sinnvoll und aus Gründen des Persönlichkeitsschutzes gefährlich.“

Thilo Weichert vom Netzwerk Datenschutzexpertise ergänzt: „Gentests liefern brisante Daten. Sie enthalten Anhaltspunkte für Erkrankungsrisiken und über Verwandschaftsbeziehungen. Das Gendiagnostikgesetz sieht bei medizinischen Genanalysen Vorkehrungen in Bezug auf Beratung und Qualität vor, damit beispielsweise das Wissen um ein genetisches Krankheitsrisiko aus einem DNA-Test wissenschaftlich korrekt bewertet und erklärt wird. Solche Vorgaben werden hier nicht eingehalten. Was genau mit den Daten geschieht, bleibt im Dunkeln. Solange Vertraulichkeit nicht gewährleistet ist, sollten Menschen – auch aus Rücksicht auf ihre biologischen Verwandten – von eigenen DNA-Tests Abstand nehmen.“



Bild: iStock

Shu-Ru Wu

E-Payment in Taiwan

A. Einleitung

Eine Statistik des zuständigen Statistischen Amtes (經濟部統計處)[1] zeigt, dass der Umsatz des Internethandels in Taiwan vom Jahr 2010 bis 2019 von 10,21 Milliarden auf 20,78 Milliarden TWD (ca. von 3 Milliarden auf 6 Milliarden Euro)[2] gestiegen ist. Die jährliche Wachstumsrate beträgt durchschnittlich 8.2%. Außerdem stieg der Anteil des Internethandels am Einzelhandel während dieses Zeitraums von 3.1% auf 5.2%. Daraus ergibt sich, dass Internethandel in Taiwan immer beliebter wird. Ob die Online-Händler passende Zahlungsmöglichkeiten anbieten, spielt daher eine große Rolle. E-Payment ermöglicht die Zahlungsabwicklung auf elektronischem Wege. Auch im stationären Einzelhandel ist E-Payment möglich. Man kann in Taiwan praktisch ohne Bargeld leben.

Dieser Artikel zeigt auf, welche Zahlungsarten des E-Payment in Taiwan bestehen und wie sie funktionieren. Außerdem wird das Gesetz über die Kontrolle der Institute für das elektronische Payment (電子支付機構管理條例)[3] und das Gesetz zur Ausstellung und Kontrolle elektronisch aufgeladener Wertkarten (電子票證發行管理條例)[4] vorgestellt. Darüber hinaus soll dieser Artikel ein Gesamtbild des E-Payment in Taiwan zeichnen.

B. Unterschiedliche Arten des E-Payment in Taiwan

E-Payment ist der Oberbegriff für den bargeldlosen Zahlungsverkehr, der sowohl beim Internetkauf als auch beim Einkauf in stationären Geschäften möglich ist. In Taiwan kann E-Payment in vier Arten eingeteilt werden, nämlich das mobile Payment, das elektronische Payment, die Zahlung durch Dritte und die Zahlung mit elektronisch aufgeladenen Wertkarten.

1. Das mobile Payment（行動支付）

Das mobile Payment wird als Zahlungsart vor allem von Girokarten- und Kreditkartenbesitzern verwendet. International bekannt sind Apple Pay, Google Pay[5] und Samsung Pay. Beim Interneteinkauf wird die Bezahlung umgehend erledigt, nachdem man das gewünschte mobile Payment gewählt hat (beim ersten Mal ist die Eingabe

der Daten der Girokarte oder Kreditkarte erforderlich). Sie dauert weniger als eine Sekunde. Anstatt die Kreditkarte mitzunehmen, kann die Bezahlung über geeignete Geräte, etwa Smartphone, Tablet-Computer und Smartwatch mit einem NFC-Chip[6] auch in stationären Geschäften vorgenommen werden. Für das kontaktlose Bezahlen legt man sein Smartphone einfach vor das NFC-Lesegerät. Der Bildschirm zeigt keine Daten der Girokarte oder Kreditkarte des Verbrauchers an. Das Bezahlen erfolgt über eine verschlüsselte Nummer, die nicht auf dem Smartphone gespeichert und bei jedem Einkauf automatisch erstellt wird. Der Händler erhält also nicht die Daten des Verbrauchers, die so geschützt werden.[7]

Das mobile Payment funktioniert nicht viel anders als die direkte Zahlung mit Girokarte oder Kreditkarte. Viele Banken in Taiwan haben hierfür ihre eigene App entwickelt.

2. Das elektronische Payment （電子支付）

Nach § 3 Abs. 1 des Gesetzes über die Kontrolle der Institute für das elektronische Payment (im Folgenden: Kontrollgesetz) werden durch die zuständige Behörde befugte Unternehmen verpflichtet, die über das Internet oder eine Plattform die Registrierung und die Eröffnung eines Kontos ermöglichen und die elektronisch das Auslösen und den Empfang von Zahlungen anbieten. Ihre Haupttätigkeiten sind die Beauftragung und der Empfang anstelle des Zahlenden oder des Empfängers, die Abwicklung von Prepaidzahlungen, die Überweisung zwischen Konten des elektronischen Payments sowie weitere zugelassene Angebote. Für Institute oder Unternehmen, die den Betrieb für das elektronische Payment leiten, ist die Financial Supervisory Commission (金管會)[8] zuständig (§ 2 des Kontrollgesetzes).

Elektronisches Payment kann auch als mobiles Payment erfolgen. Zusätzliche Services sind die Einzahlung und das Überweisen zwischen Konten des elektronischen Payments. Beide Verfahren können im Alltag kombiniert werden. Nach einer Studie des Market Intelligence & Consulting Institute (MIC) waren im Jahr 2019 LINE Pay (22.3%), Apple Pay (19.9%), JKOPay (19.7%) und Google Pay (9.1%) die beliebtesten E-Payments in Taiwan.[9] Es gibt weitere E-Payment-Angebote, etwa Garmin pay, Taiwan Pay, Pi-Wallet usw. Im Folgenden werden JKOPay und LINE Pay vorgestellt, da diese zurzeit in vielen Geschäften, Supermärkten und sogar in Nachtmärkten[10] zum Einsatz kommen.

A. JKOPay

Die JKOPay AG ist ein taiwanisches Unternehmen, das 2015 gegründet wurde und 2018 nach Erhalt der Erlaubnis den Betrieb des elektronischen Payments aufnahm. Zur Anmeldung[11] ist es erforderlich, die JKOPay App im Smartphone herunterzuladen und das eigene JKOPay-Konto mit der Bestätigung der Handynummer zu eröffnen. Das JKOPay-Konto kann entweder mit einem Bankkonto oder mit einer Kreditkarte verbunden werden. Dafür wird bei erstmaliger Verwendung die Nummer des Bankkontos oder der Kreditkarte eingegeben. Es eignet sich also auch für Personen, die keine Kreditkarte besitzen. In Bezug auf das Zahlungslimit ist entscheidend, ob man alle erforderlichen Informationen ausgefüllt hat. Bei vollständiger Ausfüllung liegt das Zahlungslimit bei maximal 300.000 TWD (ca. 8928,60 Euro) pro Monat, sonst wird es auf 30.000 TWD (ca. 892,90 Euro) beschränkt.

Für Zahlungen[12] werden zwei Möglichkeiten angeboten: Geschäfte können den Code der Karte auslesen; die Bezahlung durch Einscannen erfolgt einfach über die Karte. Es ist auch möglich, dass man seinen QR-Code vor der Kasse zum Einscannen zeigt (siehe das untere Foto), so dass über die JKOPay-App eine Überweisung ausgelöst wird. Darüber hinaus bietet JKOPay virtuelles Geld, das sog. JKO-Geld (街口幣), das unter bestimmten Bedingungen[13] mit dem echten Geld vergleichbar ist. Das kann ein Grund sein, weshalb JKOPay für immer mehr Menschen attraktiv ist.

B. LINE Pay (LINE Pay Money)[14]

Die LINE AG gehört zum südkoreanischen Unternehmen Naver AG und wurde im Mai 2013 in Taiwan als LINE Plus AG registriert. Geschäftsfelder sind die Onlinekommunikation und das elektronische Payment. Das allbekannte LINE war anfangs eine reine Kommunikations-App[15] und wurde im Jahr 2014 als LINE Pay um eine mobile Paymentfunktion erweitert. Im Paymentbereich startete die LINE AG im September 2018 eine Kooperation mit der iPass AG und dem neuen sog. LINE Pay Money.

Zur Anmeldung des LINE Pay öffnet man die LINE App und klickt auf LINE Pay. Das LINE Pay Konto muss mit der Kredit- oder Girokarte des Nutzers verbunden werden. Für die Personen, die keine Kredit- oder Girokarte haben, kann das LINE Pay-Money-Konto nach der Bestätigung der Handynummer und des Personalausweises eröffnet und genutzt werden. Wie JKOPay erfolgt das Bezahlen über LINE Pay durch Vorzeigen oder Einscannen des QR-Codes im Geschäft.[16] Anders als JKOPay gibt es bei LINE Pay weitere Funktionen, z.B. die Aufteilung einer Rechnung[17] oder die automatische Anzeige der kooperierenden Geschäfte in der unmittelbaren Umgebung des Handyinhabers mittels GPS-Daten.

Der Nutzer von LINE Pay kann auch virtuelles Geld, den sog. LINE Point, ein-

setzen. LINE Point ist für das Einkaufen oder die Bezahlung von Rechnungen für Strom, Wasser, Internet oder Handy nutzbar. LINE Pay kommt inzwischen nicht nur in Taiwan, sondern auch in Korea, Japan und Thailand zum Einsatz. Voraussichtlich noch im Jahr 2020 wird das grenzüberschreitende Zahlen für Touristen aus Korea, Japan und Thailand möglich sein, so dass diese bei Einkäufen in Taiwan keine Währung mehr tauschen müssen.

3. Zahlung durch Dritte （第三方支付）

Das Zahlen durch Dritte dient der Erhöhung der Einkaufssicherheit. Beim Einkauf im Internet kennt der Verbraucher den Verkäufer zumeist nicht. Zur Vermeidung der Nichtleistung oder nicht vertragsgemäßer Leistung wird ein Unternehmen als Dritter eingeschaltet, der das Geld des Verbrauchers aufbewahrt und dem Käufer das Geld erst übergibt, nachdem der Verbraucher die bestellten Waren erhalten und nicht beanstandet hat. Bei Zahlung durch Dritte ist PayPal[18] international das bekannteste Unternehmen. Die meisten Unternehmen in Taiwan bieten nicht nur die Zahlung durch Dritte an, sondern nach Erhalt der behördlichen Erlaubnis auch das elektronische Payment.

Nach § 3 Abs. 1 des Kontrollgesetzes sind die Institute für das elektronische Payment ausgeschlossen, wenn sie ausschließlich die Tätigkeit des § 3 Abs. 1 Nr. 1 übernehmen, also die Übernahme von Bezahlung und Empfang von Geld für Käufer und Verkäufer als Dritter. Während der Financial Supervisory Commission die zuständige Behörde für die Institute für das elektronische Payment ist, werden Unternehmen für die Tätigkeit der Zahlung durch Dritte vom Wirtschaftsministerium kontrolliert. Zur Kontrolle dieser Unternehmen hat das Wirtschaftsministerium Allgemeine Geschäftsbedingungen für die Zahlung durch Dritte beschlossen, die unverzichtbare Vertragsbedingungen sind.

4. Die elektronisch aufgeladene Wertkarte （電子票證）

Das Gesetz zur Ausstellung und Kontrolle elektronisch aufgeladener Wertkarten (im Folgenden: Ausstellungsgesetz) ist die Rechtsquelle des Services für elektronisch aufgeladene Wertkarten. Nach § 3 Nr. 1 dieses Gesetzes sind elektronisch aufgeladene Wertkarten für mehrere Zahlungszwecke verwendete Karten, die in Form eines IC-Chips, eines Zertifikats oder in anderer Form ein Schuldverhältnis nachweisen, und in denen der Geldwert in elektronischer, magnetischer oder optischer Weise gespeichert wird. In Taiwan werden sie vor allem für öffentliche Verkehrsmittel und den Kauf von Speisen und Getränken verwendet, z.B. mit der EASY Card (悠遊卡), dem iPass (一卡通) oder der Starbucks Card (星巴克隨行卡). Die elektronisch aufgeladene Wertkarte funktioniert als elektronischer Geldbeutel. Für den Service der elektronisch aufgeladenen Wertkarte ist die Financial Supervisory Commission zuständig (§ 2 des Ausstellungsgesetzes).





Wer in Taipeh mit der Metro, Bus oder Zug fahren möchte, kann mit der EASY Card das Ticket bezahlen, in Kaohsiung[19] mit dem iPass. Vor der Zahlung ist darauf zu achten, dass Geld auf die Karte geladen wurde. iPass bietet seit der Kooperation mit der LINE AG im Jahr 2018 zudem den Service für das elektronische Payment an. Die EASY Card AG will dem folgen; sie hat bereits im Jahr 2019 die Erlaubnis für das elektronische Payment erhalten und angekündigt, Ende März 2020 den Service für das elektronische Payment zu starten.

C. Die geltenden Gesetze und die Diskussion über E-Payment

E-Payment wird in Taiwan immer beliebter. Es ist praktisch und macht den Alltag im Zahlungsverkehr bequemer. Trotzdem stehen einige Fragen zur Diskussion:

1. Zunächst der Datenschutz: Eine Umfrage des MIC über E-Payment vom Jahr 2017 hat ergeben, dass 80,2 % der Verbraucher bereit sind, E-Payment zu benutzen. Allerdings äußerten auch 82,3 % der Befragten Bedenken wegen der Sicherheit.[20] Dabei geht es um die Zahlungssicherheit sowie um den Schutz der Nutzerdaten etwa bei Verlust der Geräte (z. B. Smartphones). Die Financial Supervisory Commission als zuständige Behörde hat gemäß § 29 II des Kontrollgesetzes den Standard des Informationssystems und der Sicherheitskontrolle für Institute des elektronischen Payment (電子支付機構資訊系統標準及安全控管作業基準辦法)[21] festgelegt. Dieser Standard umfasst zahlreiche technische Anforderungen, wie etwa die Verfahren zur Registrierung, die Verfahren zur Bestätigung des Nutzers beim Einloggen und die Regelung über Einstellung der Schlüsselwörter. Stellen die Unternehmen den Verbrauchern eine dem Standard nicht entsprechende Betriebsumgebung zur Verfügung, so können sie wegen eines Verstoßes gegen § 29 II des Kontrollgesetzes zur Zahlung eines Zwangsgeldes in Höhe von 600.000 bis zu 3 Millionen TWD (ca. von 17.857 bis zu 89.285 Euro) verpflichtet werden.
   Sicherheit ist nicht nur die Angelegenheit der Unternehmen oder Anbieter des Services, sondern fordert auch die Kooperation der Nutzer des E-Payment. Risiken können reduziert werden, indem die Nutzer eine Displaysperre auf ihrem Smartphone oder sonstigen Gerät einrichten und dieses sorgfältig aufbewahren. Die Passwörter müssen häufig verändert werden. Außerdem ist zu vermeiden, dass unbekannte Apps heruntergeladen werden; nicht verwendete Apps sind zu deinstallieren.
2. Zudem ist Geldwäsche ein Thema. Zwar sind die Unternehmen keine

Banken, doch führen auch sie Überweisungen aus. Dies macht es notwendig, bei Eröffnung des Kontos des elektronischen Payments die Identität des Nutzers durch Handynummer und Nummer des Personalausweises zu bestätigen. Zudem besteht die Gefahr, dass Angestellte der Unternehmen mit Zugang zu den Kundendaten diese an Werbeträger oder andere Firmen verkaufen. Auch die unbefugte Weitergabe an Kreditprüfungsunternehmen ist ein Risiko. Zur Vermeidung von Betrug und Untreue wird von den Unternehmen ein internes Kontrollsystem gefordert (compliance).

3. Die Politik sollte für eine Vereinheitlichung des elektronischen Payments sorgen. Die Überweisung zwischen den Konten verschiedener Banken ist kostenpflichtig problemlos möglich. Allerdings nicht machbar ist es, dass z.B. ein Nutzer des JKO Pay eine Überweisung auf ein LINE Pay-Konto vornimmt. Mit einer Vereinheitlichung des elektronischen Payments soll künftig das Überweisen zwischen Konten verschiedener Anbieter möglich sein; zugleich steht die Vereinheitlichung des Kontrollgesetzes und des Ausstellungsgesetzes auf der Agenda.[22]

D. Fazit

Bargeldlose Bezahlung ist seit dem Jahr 2015 eines der Hauptziele der Financial Supervisory Commission. E-Payment soll als praktische Zahlungsart den Binnenmarkt beleben und es Touristen weltweit erleichtern, nach Taiwan zu kommen und hier zu reisen.

Laut der Statistik der Financial Supervisory Commission[23] beträgt bis zum Ende Januar 2020 die Zahl der Nutzer des elektronischen Payments 7,26 Millionen. Gegenüber Dezember des Jahres 2019 ist diese Zahl um 340.000 gestiegen. Es wurden 12,76 Millionen elektronisch aufladbare Wertkarten benutzt. Im Vergleich zum Dezember des Jahres 2019 ist dies eine Zunahme um 1,46 Millionen. Eine weitere Zunahme ist zu erwarten. Damit ersetzt E-Payment das Bargeld nicht und bietet in Taiwan hierzu eine Zahlungsalternative.

1 Die Statistik 2: Der Einzelhandelsumsatz (表2：零售業營業額), siehe: https://www.moea.gov.tw/Mns/dos/bulletin/Bulletin.aspx?kind=8&html=1&menu_id=6727&bull_id=6744, Stand: 15.3.2020.

2 TWD ist die Abküzung des Taiwan-Dollars. Der Wechselkurs des Euro in TWD beträgt ca. 1 zu 33,6. https://www.umrechner-euro.de/umrechnung-taiwan-dollar, Stand: 15.3.2020.

3 The Act Governing Electronic Payment Institutions abrufbar unter: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380237, Stand: 15.3.2020.

4 The Act Governing Issuance of Electronic Stored Value Cards abrufbar unter: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380207, Stand: 30.3.2020.

5 Die Vorstellung von Google Pay in Deutschland ist abrufbar unter: https://pay.google.com/intl/de_de/about/

6 NFC ist die Abkürzung für Nahfeldkommunikation. Sie ist eine technische Methode für die Datenübertragung und der NFC-Chip dient dem kontaktlosen Datenaustausch auf kurzer Distanz.

7 Der Film: Wie bezahle ich mit Google Pay in Geschäften? https://www.youtube.com/watch?v=o69mkycAQKQ&feature=emb_logo, Stand: 15.3.2020.

8 Die Financial Supervisory Commission (abgekürzt FSC) unterliegt dem Executive Yuan (行政院). Der Executive Yuan ist die höchste Behörde für Verwaltung Taiwans. Nach § 2 Organisationsgesetz des Financial Supervisory Commission ist FSC die zuständige Behörde für die Entwicklung, Überwachung, Regulierung und Kontrolle der Finanzmärkten und der Finanzdienstleistungsunternehmen. Die englische Version des Organisationsgesetzes des Financial Supervisory Commission ist abrufbar unter: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0300035, Stand: 29.3.2020.

9 Studie über Verbraucher des E-Payment (行動支付大調查): https://mic.iii.org.tw/news.aspx?id=551, Stand: 22. 3. 2020.

10 Nachtmärkte sind Teil der taiwanischen Kultur, in denen viele Stände verschiedene Speise und Getränke anbieten, ebenso Schmuck, Kleidung und interessante Dinge zu günstigen Preisen. Von Nord- bis Südtaiwan gibt es zahlreiche Nachtmärkte; bekannt und in Reiseführer zu finden sind z.B. Shida-Nachtmarkt (師大夜市), Shilin-Nachtmarkt (士林夜市), Raohe-Nachtmarkt (饒河夜市).

11 Die Vorstellung über die Anmeldung bei JKOPay, https://www.jkopay.com/instructions/register.html, Stand: 17.3.2020.

12 Die Vorstellung über die Bezahlung per JKOPay, https://www.jkopay.com/instructions/pay.html, Stand: 28.3.2020.

13 Ein JKO Geld ist gleich ein TWD. Bei Einkäufen kann man mit JKO Geld maximal 30% TWD eintauschen.

14 Webseite von LINE Pay, https://pay.line.me/portal/global/main, Stand: 15.3.2020.

15 LINE als ein Kommunikationsmittel wird für Kontakte mit Freunden, Familien, aber auch in der Arbeitswelt verwendet. Es wird diskutiert, ob der Arbeitgeber nach der Arbeit Arbeitnehmer über LINE zu Tätigkeiten verpflichten kann.

16 Die Vorstellung über die Bezahlung per LINE Pay, https://pay.line.me/portal/global/business/payment-service, Stand: 28.3.2020.

17 Beim Treffen mit Freunden bezahlt man normalerweise getrennt in Taiwan; wegen der Probleme beim Aufteilen der Rechnung kann so eine Lösung gefunden werden.

18 Webseite von PayPal, https://www.paypal.com/de/webapps/mpp/personal, Stand: 28.3.2020.

19 Kaohsiung ist eine der größten Städte Taiwans und liegt in Südtaiwan.

20 Die Untersuchung der Verbraucher für das E-Payment (行動支付消費者調查), https://mic.iii.org.tw/news.aspx?id=457, Stand: 9.4.2020.

21 Regulations Governing the Standards for Information System and Security Management of Electronic Payment Institutions abrufbar unter: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380243, Stand: 1.4.2020.

22 Entnommen der Zeitung Anue: Das Nichtzustandekommen der Gesetzvereinheitlichung (台灣電子支付大整合卡關), https://news.cnyes.com/news/id/4404482, Stand: 1. 4.2020.

23 Die Statistiken über der Informationen der Kredit- und Geldkarte, der elektronisch aufgeladenen Wertkarte und des elektronischen Payment (109年1月份信用卡、現金卡、電子票證及電子支付機構業務資訊) , siehe: https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202003050003&toolsflag=Y&dtable=News, Stand: 1.4.2020.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Kontodatenabfragen steigen weiter

Staatliche Stellen, also Behörden und Gerichtsvollzieher, machen weiter sehr rege von ihrer Befugnis Gebrauch, Kontodaten, also Stammdaten von Konteninhabern, bei Banken und Sparkassen abzufragen. Im Jahr 2019 haben gemäß einer Mitteilung des Bundesfinanzministeriums Ämter und Gerichtsvollzieher in 915.257 Fällen Einsicht beantragt. Das ist ein Plus von knapp 15% gegenüber dem Vorjahr. Die Zahl der Kontendatenabfragen ist insbesondere seit 2013 stetig angestiegen. Nutzten die berechtigten Institutionen das Instrument 2012 noch 72.000 Mal, waren es 2017 schon 692.000 Anträge.

Der Bundesdatenschutzbeauftragte Ulrich Kelber sieht die jährlich rasant steigende Nachfrage kritisch: „Jeder Kontenabruf stellt einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar." Er bezweifelt, dass das Werkzeug angesichts der regelmäßigen Steigerungen noch verhältnismäßig eingesetzt wird, und fordert die Bundesregierung nachdrücklich auf, das Verfahren zu evaluieren. Er erinnerte daran, dass der Gesetzgeber den automatisierten Abruf von Kontoinformationen als Folge der Terroranschläge von 2001 eingeführt habe, um Geldwäsche und Terrorismusfinanzierung besser bekämpfen zu können. Zunächst durfte nur die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) Kontenabfragen für die Sicherheitsbehörden durchführen. Seit 2005 darf das Bundeszentralamt für Steuern (BZSt) Einsicht beantragen, 2013 kamen Gerichtsvollzieher hinzu und 2017 Verwaltungen, die etwa Ausbildungsförderung oder Wohngeld genehmigen.

Für Kelber ist damit aus einem Instrument zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung ein Vollstreckungshilfsmittel geworden. Angesichts des damit verknüpften Grundrechtseingriffs müssten Gesetzgeber und Behörden aber „alles tun, um dieses Instrument maßvoll einzusetzen". Es dürfe etwa nicht zu Personenverwechslungen kommen, „weil Schuldner und vermeintlicher Schuldner zufällig denselben Namen tragen". Solche Fehler verletzten den datenschutzrechtlichen Grundsatz der Integrität und Vertraulichkeit und seien für die Betroffenen nicht hinnehmbar. Er begrüßt es zwar, dass der Bundestag mit dem Steuerumgehungsbekämpfungsgesetz beim Schutz von Kontendaten etwas nachgebessert habe. Es bleibe aber abzuwarten, ob diese Korrekturen „tatsächlich greifen". Kelbers Vorgängerin Andrea Voßhoff hatte 2018 ebenfalls bereits konstatiert, dass das Werkzeug schleichend ausgeweitet worden sei und daher dringend überprüft werden müsse. Fehler könnten im Einzelfall äußerst unangenehme Folgen wie Kontensperrungen nach sich ziehen (vgl. z.B. DANA 2014, 26, 76; Krempl, Gläserner Bankkunde: Kontenabfragen erreichen neuen Höchststand, www.heise.de 30.01.2020, Kurzlink: https://heise.de/-4649686).

Bund

CCC-Experten enttarnen FinFisher-Überwachungssoftware

In einem auf dem 36. Chaos Communication Congress (36C3) in Leipzig veröffentlichten Bericht haben Experten des Chaos Computer Clubs (CCC) im Auftrag der Gesellschaft für Freiheitsrechte (GFF) mehrere Trojaner-Samples der deutschen Firma FinFisher von 2012 bis 2019 eingehend untersucht und nachgewiesen, dass der mutmaßlich von der türkischen Regierung gegen Oppositionelle eingesetzte Android-Trojaner von der Münchner Firma Gamma International/FinFisher stammt. Außerdem sehen sie es als erwiesen an, dass das von ihnen untersuchte Schadcode-Sample nach dem 18.07.2015 erstellt wurde.

Darin läge ein Verstoß gegen § 18 Außenwirtschaftsgesetz (AWG), wenn Berichte der Bundesregierung vom Juli 2019 zutreffen, dass für Staatstrojaner bisher keine entsprechenden Genehmigungen erteilt wurden. Dies hätte wiederum zu Folge, dass den zuständigen FinFisher-Mitarbeitern eine Freiheitsstrafe von bis zu fünf Jahren droht. Netzpolitik.org, die GFF, Reporter ohne Grenzen und das European Center for Constitutional and Human Rights haben deshalb Strafanzeige beim zuständigen Zollkriminalamt gestellt. Das Schadprogramm wurde gegen Mitglieder der türkischen Opposition eingesetzt.

Thorsten Schröder und Linus Neumann vom CCC haben Ähnlichkeiten zu veröffentlichten Schadcode-Samples aufgezeigt, die bekanntermaßen der Münchner Firma zuzuordnen sind. Als Vergleichsmaterial diente ihnen für ihren Bericht das Material, das bei einem Systemhack von FinFisher im Jahr 2014 öffentlich wurde. Dabei veröffentlichte Schadcode-Samples stammen erwiesenermaßen von den Entwicklern der Münchener Firma und konnten nun mit dem Schadcode-Sample namens adalet verglichen werden, das von der Webseite adaleticinyuru.com stammt, welche gemäß der GFF-Strafanzeige türkische Oppositionelle dazu verleiten sollte, diesen Schadcode zu installieren. Schröder und Neumann sehen es als erwiesen an, dass die Ähnlichkeiten der aus dem FinFisher-Leak stammenden Samples und dem adalet-Sample nicht zufällig sind und dass adalet somit von den FinFisher-Entwicklern stammt und eine Weiterentwicklung des FinSpy-Android-Trojaners ist. Insgesamt untersuchten sie 28 Schadcode-Samples, die alle von der Münchener Firma stammen sollen und nach Ansicht der CCC-Experten eine

Entwicklung der Spionage-Software des Herstellers von 2012 bis 2019 aufzeigen.

Obwohl die CCC-Experten in ihrer Analyse nach dem Hack bei FinFisher und dem daraus resultierenden Datenleck im Jahr 2014 Bemühungen der Münchener Firma feststellen, ihren Quellcode zu refaktorisieren und mittels Obfuscation unkenntlich zu machen, blieben wichtige Eigenschaften der FinSpy-Trojaner-Familie auch danach funktionell erhalten. Anti-Viren-Hersteller hatten nach dem Datenleck bei FinFisher ihre Erkennungsroutinen an den Schadcode angepasst, um ihn und ähnliche Codes entdecken zu können. Die Münchener Entwickler änderten danach ihre Software dann wohl, um der Entdeckung ihres Trojaners durch AV-Programme wieder zu entgehen. Allerdings konnten sie ihren Code nicht allzu sehr funktional ändern, ohne große Teile davon neu zu entwickeln. Entsprechend sind die Trojaner-Sample vor und nach 2014 trotz äußerlicher Änderungen funktional sehr ähnlich. Das wird besonders deutlich, wenn man die logischen Abläufe der zu vergleichenden Samples mit einem Code-Flow-Diagramm kartiert.

Laut dem Bericht der CCC-Experten enthalten die untersuchten Samples allesamt einen weitgehend funktionell seit 2012 unverändert gebliebenen Mechanismus, um den Trojaner für seinen Einsatz zu provisionieren, also um eine auf den jeweiligen Kunden der Firma FinFisher angepasste Konfiguration auszurollen. Auf diese Weise wird der Trojaner für eine konkrete Spionage-Mission vorbereitet. Um diese Konfigurationsdaten möglichst unauffällig zu halten, nutzen die FinFisher-Entwickler einen verdeckten Kanal, indem sie ihre Konfigurations-Parameter in Dateiattributen des Android-Paketformates APK versteckten.

APK-Dateien sind im Grunde .ZIP-Archive und sehen laut ihrer Spezifikation für jede in dem Archiv enthaltene Datei bestimmte Felder vor, in die Dateiattribute kodiert werden; dabei handelt es sich um Metadaten zu der jeweiligen Datei. APK-Archive können auch leere Dateien enthalten und auch für diese sind Dateiattribute gespeichert. Laut Schröder und Neumann entwickelte FinFisher für die FinSpy-Trojaner-Familie eine Kodierung, die zum Provisioning des Trojaners benötigte Daten als solche Metadaten im APK enthaltener Dateien hinterlegt. Spezieller Code der Software, offensichtlich eine proprietäre Entwicklung der Münchener, liest diese Metadaten aus und dekodiert sie als Konfigurationsinformationen für den Trojaner. Dieser Kodierungsmechanismus wurde augenscheinlich kontinuierlich weiterentwickelt, ist im Grunde aber bei allen untersuchten Samples vorhanden. Im Rahmen der Veröffentlichung ihres Untersuchungsberichtes stellen die Autoren neben den analysierten Samples auch die von ihnen entwickelten Software-Werkzeuge bereit, mit denen sich aus den vorhandenen Samples die Konfigurationsdaten auslesen lassen.

In den im Bericht vollständig abgebildeten Konfigurations-Daten aller untersuchter Samples finden sich unter anderem verschiedene Subdomains der Domain gamma-international.de, deutsche Handy-Nummern und eine Münchener Festnetznummer. Anscheinend handelt es sich hierbei um den Command-and-Control-Rückkanal, über den die Software die Ergebnisse ihrer Spionage an den Hersteller zurückschickt. Einige der Samples wurden mit Telefonnummern oder Domains unter anderem in Vietnam konfiguriert. Vietnam wurde ebenso wie die Bundesregierung in der Vergangenheit immer wieder als Kunde mit FinFisher in Verbindung gebracht. Neben diesen Hinweisen auf die Münchener Firma dokumentieren die CCC-Experten auch noch weitere Eigenarten des FinSpy-Codes, der darauf hindeutet, dass hier deutsche Entwickler am Werk waren.

In den Konfigurationsdaten sind Trojaner-Funktionen wie „Spy Call", „Call Interception", „Tracking" und „Phone Logs" erwähnt, die über Parameter an- und abgeschaltet werden können. Weitere Parameter scheinen zu steuern, wie viele Geräte der Trojaner maximal infizieren darf und unter welchen Bedingungen die Konfigurationsdaten des Trojaners zu löschen sind. Ein Trojaner-Sample enthält darüber hinaus weitere externe Dateien, die wohl die Privilege-Escalation-Schwachstelle für den Linux-Kernel DirtyCow ausnutzen sollen und Android-Smartphones darüber hinaus mit dem Software-Tool SuperSU rooten können. Diese FinSpy-Variante ist anscheinend dafür gedacht, weitere Schadsoftware auf dem betroffenen Gerät zu platzieren.

Schröder und Neumann sehen es mit an Sicherheit grenzender Wahrscheinlichkeit als erwiesen an, dass das aus der Türkei stammende adalet-Sample von denselben Entwicklern wie bekannte FinSpy-Samples stammt. Im nächsten Schritt ging es ihnen darum, zu beweisen, dass der Schadcode nach dem 18.07.2015 erstellt wurde. Das schließen sie vor allem aus der in dem besagten Trojaner-Sample verwendeten Version der Datenbank-Software SQLite. Die der Software beiliegende SQLite-Bibliothek ist die Version 3.13.0, die am 18.05.2016 veröffentlicht wurde. Außerdem wurde die adalet-APK mit einem Zertifikat signiert, das ab dem 10.10.2016 gültig ist. Kompiliert wurden Teile des Codes augenscheinlich am 23.09.2016. Es kann also davon ausgegangen werden, dass dieses Sample nach dem 18.05.2016 fertig gestellt wurde und erst nach dem 10.10. des selben Jahres zum Einsatz kam.

Der von den CCC-Experten nach eigenen Angaben ehrenamtlich angefertigte Bericht ist unter dem Titel „Evolution einer privatwirtschaftlichen Schadsoftware für Staatliche Akteure" veröffentlicht. Die Analyse, alle darin untersuchten Software-Samples und die zum Auslesen der Trojaner-Konfiguration entwickelten Tools stehen auf GitHub zur Verfügung. Interessierte Mitglieder der IT-Security-Gemeinde werden so ausdrücklich dazu aufgefordert, die veröffentlichten Forschungsergebnisse zu prüfen (Scherschel, 36C3: Spionage-Trojaner FinFisher – CCC weist rechtswidrigen Export nach, www.heise.de 28.12.2019, Kurzlink: https://heise.de/-4624098).

Bund

„Stiftung Datenschutz" vor dem Aus

Die Stiftung Datenschutz mit Sitz in Leipzig steht finanziell als Spielball der Bundestagsfraktionen CDU/CSU, SPD und FDP vor dem Aus. Sie versteht sich als Bindeglied zwischen Bußgeldbehörden und Unternehmen, so Frederik Richter, der Leiter der Stiftung: „Was uns

auszeichnet, ist Äquidistanz zwischen Aufsicht und Wirtschaft, das kann eine Aufsicht nicht machen". Wenn die Stiftung kein Geld mehr erhält, brechen die rot-schwarzen Regierungsparteien ein Versprechen ihres Koalitionsvertrags: „Wir wollen die Arbeit der Stiftung Datenschutz fördern." Der Stiftung geht jetzt das Geld aus. Richter hat zum zweiten Mal bei der Aufsicht beantragt, auf das Stiftungsvermögen zugreifen zu können, da die eigenen Einnahmen nicht ausreichen, und er hat die Genehmigung zur Überraschung mancher wenig wohlwollender Beobachter auch erhalten. Ihm bleiben gerade einmal 80.000 Euro für die Arbeit. Das sächsische Recht sieht diese Möglichkeit für im Land angesiedelte Stiftungen vor. Doch der vom Bundesinnenministerium dominierte Verwaltungsrat hat die Zustimmung verweigert. Richters Vertrag lief Ende 2019 aus; seitdem führt er kommissarisch die Geschäfte.

Ein Geburtsfehler der im Jahr 2013 gegründeten Stiftung ist, dass sie damals von der sozialliberal eingestellten Justizministerin Sabine Leutheusser-Schnarrenberger (FDP) gegen den damals für Datenschutz zuständigen konservativen Innenminister Hans-Peter Friedrich (CSU) durchgesetzt wurde. Wegen der Dauerverweigerung der FDP bei der Telekommunikations-Vorratsdatenspeicherung hatten manche sogar zeitweise einen Koalitionsbruch befürchtet. Daran erinnere man sich auch im Bundesinnenministerium noch recht gut, so FDP-Bundestagsabgeordneter Stefan Ruppert: „Mir scheinen die Animositäten gegenüber der Stiftung noch aus dieser Zeit herzurühren." Die Organisation werde dort als „Fremdkörper" wahrgenommen – nicht auf Ebene der Parlamentarischen Staatssekretäre, sondern in der Fachabteilung. Diesen Eindruck hört man auch aus der Union selbst. Es handele sich um ein Versorgungswerk für die „Gelben", zumal der Stiftungsleiter Richter früher FDP-Referent war.

Es scheint wenig zu nützen, dass die Stiftung Veranstaltungen zu SPD-Themen organisiert, wie die Datenteilungspflicht, und ihre Arbeit parteiübergreifend bei Digitalpolitikern gelobt wird. Das Bundesinnenministerium will, so Ruppert, die Stiftung auch nicht an das Justizressort abgeben oder an die Behörde des Bundesdatenschutzbeauftragten (BfDI) Ulrich Kelber. Kelber würde die Stiftung zwar gerne übernehmen, benötigt dann aber hierfür auch Haushaltsmittel.

In der SPD will der Haushaltspolitiker Johannes Kahrs offenbar den letzten Rest gelber Farbe aus dem Wirkbereich der Bundesregierung kratzen. Der Stiftung werde „kein Euro gestrichen", erklärte er auf Medienanfrage am Telefon; im Übrigen kenne er sich im Bereich Datenschutz gar nicht so gut aus. In einem Streit mit der Stiftung auf Twitter war der Politiker zuvor rabiater und hatte ihr „Lügen" vorgeworfen. Tatsächlich war es das Innenressort, das in Haushaltsentwürfen für die letzten drei Jahre die Förderung eingestellt hatte.

Dennoch spielte Kahrs im Verdeckten die entscheidende Rolle. Zunächst hatte es gut ausgesehen für die Stiftung: Politiker der FDP hatten in der Union dafür geworben, die Stiftung im Rahmen der Bereinigungssitzung zu fördern und sie vor allem nicht abzuwickeln. Denn sogar für das formale Ende lag zwischenzeitlich ein Plan auf dem Tisch. Im Rahmen des Feilschens in Haushaltssitzungen können auch Oppositionsparteien das eine oder andere durchsetzen. Nun sollte es ein stiller Erfolg der FDP sein, die Stiftung vor der Abwicklung zu retten und am Leben zu halten. Ersteres gelang: Der Maßgabebeschluss zur Abwicklung verschwand wieder. Zweiteres misslang: Obwohl die Förderung auf einem Deckblatt festgeschrieben stand, verschwand dies wieder.

Der hessische FDP-Vorsitzende Ruppert, der sein Bundestagsmandat im Frühjahr 2020 aufgibt und als Personalvorstand bei B. Braun antritt, berichtete, sein Gesprächspartner auf Unionsseite habe ihm zerknirscht mitgeteilt, Kahrs wolle eine „Trophäe aus schwarz-gelber Zeit". In der CDU habe man das dann hingenommen. Die unterbliebene Finanzierung sei „eine der traurigsten Erfahrungen, die ich gemacht habe". Er schließt jedoch hoffnungsvoll: „Man sollte noch einen neuen Anlauf machen, damit das nicht das letzte Wort ist."

BfDI Kelber (SPD) ist für die Fortsetzung der Stiftungsarbeit: „Ich würde begrüßen, wenn die Stiftung finanziell in die Lage versetzt würde, dauerhaft ihre Rolle als Dialogplattform erfüllen zu können." Er sieht die in ihren Stellungnahmen durchaus wirtschaftsfreundlichere Stimme im Chor der Datenschützer als willkommen an – und nicht als Gegenspieler. „Die Stiftung Datenschutz und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit stehen nicht in Konkurrenz zueinander. Beide Institutionen arbeiten in unterschiedlichen Aufgabenfeldern, unsere Arbeit ergänzt sich."

Gemäß dem Stiftungsleiter Richter hat das Bundesinnenministerium als für den Datenschutz zuständiges Ressort kein großes Interesse mehr an der Stiftung. Dabei hatte die Bundesregierung noch bis vor kurzem stolz auf die Stiftung verlinkt: „Wenn die Ministerialbeamten es in den Beschlussvorschlag geschrieben hätten, wäre die Finanzierung dringeblieben. Ich rechne mit allem, kämpfe aber bis zum Schluss für das Projekt" (Wieduwilt, Stiftung Datenschutz vor dem Aus, www.faz.net 14.01.2020).

Bundesweit

Datenleck beim HIS

Wegen eines Konfigurationsfehlers der Hochschul-Informationssysteme (HIS) standen persönliche Daten von hunderttausenden Studierenden über Jahre offen im Netz. Die Systeme der HIS Hochschul-Informations-System eG werden von zahlreichen deutschen Universitäten genutzt. Durch eine fehlerhafte Berechtigungsprüfung war es möglich, persönliche Daten hunderttausender Studierender per Browser abzufragen, darunter Name, Adresse, Matrikelnummer, Geburtsdatum und Immatrikulationsstatus. Die HIS eG wurde nach eigenen Angaben am 06.03.2020 vom Administrator einer betroffenen Hochschule auf die Sicherheitslücke hingewiesen.

Man habe, so das Unternehmen, noch am selben Tag einen Workaround an die eigenen Kunden kommuniziert und am 09.03.2020 ein Sicherheitsupdate zur Verfügung stellt. Doch nicht alle Universitäten spielten das Update der HIS eG unverzüglich ein. Bei einer Überprüfung am 12.03.2020 von insgesamt 58 Hochschulen waren noch mehrere anfällige Systeme zu finden. Daten von

über 600.000 Studierenden der Universitäten in Bonn, Düsseldorf, Hildesheim und dem Saarland waren online abrufbar, wofür allein die Kenntnis der URL genügte. Die Daten reichten vom Wintersemester 1991/92 bis zum aktuellen Sommersemester 2020. Nachdem die vier Universitäten hierüber informiert worden waren, schlossen auch sie noch am selben Tag die Lücke.

Normalerweise sollten nur bestimmte Mitarbeiter der Uni die betroffenen Informationen abfragen können. Durch den Fehler erfolgte jedoch keine solche Prüfung der Zugangsberechtigung. Laut Angaben der HIS eG bestand die Lücke seit 2011. Wie viele Universitäten und Studierende von der Lücke betroffen waren, konnte das Unternehmen auf Nachfrage nicht mitteilen: Man habe alle potentiell betroffenen Kunden informiert, aber nicht alle Kunden würden die fehlerhafte Komponente des Systems auch tatsächlich einsetzen. Inwieweit Unbefugte während der neun Jahre auf die Daten zugegriffen haben, ließ sich nach Angaben der HIS eG und der kontaktierten Universitäten nicht mehr nachvollziehen: Log-Dateien, die entsprechende Zugriffe protokollieren, reichen üblicherweise nur ein bis vier Wochen zurück. Betroffen könnten also alle Studierenden jeder Hochschule sein, die das System der HIS eG seit 2011 einsetzt oder eingesetzt hat.

Die Namen, Adressen und Geburtsdaten lassen sich zum Identitätsdiebstahl missbrauchen. Über die Matrikelnummern ließen sich auch Noten und Beurteilungen zuordnen, die an Unis – zumindest früher – oft öffentlich aushingen. Ebenso ließe sich über den Immatrikulationsstatus unter anderem nachvollziehen, wann und bis zu welchem Semester eine Person an einer Uni studiert hat.

Gemäß der DSGVO müssen die betroffenen Universitäten die in ihrem Land zuständigen Datenschutzbehörden umgehend über die Lücke informieren. Die von dem Magazin c't kontaktierten Hochschulen gaben an, das unverzüglich getan zu haben. Als Grund für die lange Speicherung von fast 30 Jahren teilten sie mit, dies sei zum Nachweis von Studien- und Versicherungszeiten nötig. Die betroffenen Studierenden wären von den Hochschulen direkt zu informieren, wenn von dem Datenleck eine „erhebliche Gefahr" ausgeht, worüber letztlich die jeweiligen Datenschutzaufsichtsbehörden entscheiden. Bußgelder gegenüber den staatlichen Hochschulen sind per Gesetz nicht vorgesehen. Möglich wären aber Schadenersatzansprüche der Betroffenen. Nötig hierfür wäre aber der Nachweis eines tatsächlichen Schadens. Die HIS eG erklärte, mit jedem Release „umfangreiche Qualitätssicherungsmaßnahmen" durchzuführen, ergänzt durch „regelmäßige Sicherheitsüberprüfungen durch externe Spezialisten", was offenbar aber hier nicht geholfen hat. Die Universitäten müssen sicherstellen, dass sicherheitsrelevante Patches künftig umgehend eingespielt werden (Tremmel, Datenleck an Hochschulen, www.heise.de 17.03.2020, Kurzlink: https://heise.de/-4683940).

Bundesweit

Datenschutzbedenken gegen Glückspiel-Staatsvertrag

Der frühere Bundesdatenschutzbeauftragte Peter Schaar kritisiert die geplante Reform des Glücksspielstaatsvertrags als unverhältnismäßige „fürsorgliche Beobachtung durch den Staat": „Was als Schutz vor der Spielsucht gedacht ist, führt zur Totalüberwachung und Bevormundung." Die Zielsetzungen, die die Länder mit dem Entwurf verfolgten, seien zwar prinzipiell richtig und nachvollziehbar. Es bestünde ein öffentliches Interesse, den Gefahren von Spielsucht entgegenzuwirken und Geldwäsche zu bekämpfen. Doch seien die vorgesehenen Regeln aus Datenschutzsicht „mehr als bedenklich" und mit der Datenschutz-Grundverordnung (DSGVO) nicht vereinbar. Die geplante zentrale Spielerdatei sei nichts anderes als eine anlasslose zentrale Vorratsdatenspeicherung, beklagt Schaar, der Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) ist. Er hat seine Kritik in einem Gutachten für den Deutschen Verband für Telekommunikation und Medien (DVTM), dem viele Unternehmen der Glücksspielbranche angehören, festgehalten.

Die Länder hatten im Januar 2020 nach jahrelangen Verhandlungen über die Novelle des Glücksspielmarktes einen Durchbruch erzielt. Bisher illegale Online-Casinos sollen demnach grundsätzlich erlaubt werden. Im Interesse des Spielerschutzes soll aber eine monatliche Einzahlgrenze von 1.000 € im Internet sowie eine zentrale Datei für Sperren und zur „Limitüberwachung" eingeführt werden. Auch die nordrhein-westfälische Datenschutzbeauftragte Helga Block äußerte Bedenken wegen der hohen „Streubreite" der Maßnahmen. Sie kritisiert, dass es laut dem Entwurf nicht mehr möglich sein werde, anonym online zu wetten. Jeder Vorgang würde künftig auf einem personengebundenen Spielerkonto registriert. Die Anbieter müssten Daten aller Teilnehmer an Sportwetten erheben und speichern. Nicht alle davon hätten Suchtprobleme.

Der hessische Innenminister Peter Beuth (CDU) warnte ebenso vor einem zu großen Überwachungsapparat und dem „gläsernen Spieler". In der Bevölkerung trifft die ausgemachte Reform ebenfalls auf Widerspruch: 60% der Bundesbürger halten, so eine repräsentative Dimap-Umfrage, das Einsatzlimit für zu streng. Besonders ablehnend stehen demnach Anhänger der AfD, der FDP und von CDU/CSU mit Quoten zwischen 74 und 60% dem Vorhaben gegenüber. Die 16 Gesellschaften des Deutschen Lotto- und Totoblocks (DLTB) begrüßten die Einigung dagegen. Es gehe darum, mit den neuen Vorschriften den illegalen Markt im Online-Bereich zurückzudrängen (Krempl, Glücksspielstaatsvertrag: Datenschützer warnt vor Totalüberwachung, www.heise.de 25.02.2020, Kurzlink: https://heise.de/-4667792).

Bayern

Will folgt Kranig

Michael Will wurde zum 01.02.2020 für die Dauer von fünf Jahren zum Präsidenten des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) und damit zum Nachfolger von Thomas Kranig ernannt.

Will wurde 1968 in Kronach geboren und ist Vater eines Kindes. Nach

dem Studium der Rechtswissenschaft in Würzburg und der Referendarzeit in Bamberg begann er im Jahr 1995 bei der Regierung von Oberfranken in Bayreuth seine berufliche Tätigkeit als Verwaltungsjurist in den Diensten des Freistaats Bayern. Nach seinem Wechsel in die Oberste Baubehörde im Bayerischen Staatsministerium des Innern im Jahr 1997 und im Jahr 2000 in die Bayerische Staatskanzlei übernahm Michael Will 2002 die Leitung der Abteilung für öffentliche Sicherheit und Ordnung im Landratsamt Landshut. Zugleich war er in dieser Zeit Geschäftsführer des Zweckverbands für Rettungsdienst und Feuerwehralarmierung Landshut. 2006 kehrte er als Referent in das Sachgebiet Straßenrecht in die Oberste Baubehörde im Bayerischen Staatsministerium des Innern zurück.

2009 wurde Michael Will die Leitung des Referats „Datenschutz" im Bayerischen Staatsministerium des Innern für Sport und Integration übertragen. Er übte dort zudem das Amt des behördlichen Datenschutzbeauftragten aus und war Mitglied der Datenschutzkommission des Bayerischen Landtages. Im Auftrag des Bundesrates begleitete er in den Jahren 2012 bis 2015 die gesamten Beratungen der Ratsarbeitsgruppe Datenschutz und Informationsaustausch (DAPIX) zur EU Datenschutz-Grundverordnung (DSGVO) und nahm außerdem die Aufgaben des Länderbeobachters im Ausschuss nach Art. 93 der DSGVO wahr, der z.B. beim Erlass von Adäquanzentscheidungen der Europäischen Kommission beteiligt wird (https://www.lda.bayern.de/de/praesident.html).

Brandenburg

Datensicherheitslücke beim Roten Kreuz

Daten zu mehr als hunderttausend Einsatzfahrten und mehr als 30.000 Patientinnen und Patienten des Deutschen Roten Kreuzes (DRK) in Brandenburg sind offenbar jahrelang auf einem schlecht gesicherten Server leicht zugänglich gewesen, darunter auch sensible Gesundheitsinformationen aus Aufzeichnungen des DRK-Kreisverbands Märkisch-Oder-Havel-Spree, zu dem Orte wie Eisenhüttenstadt, Frankfurt (Oder), Oranienburg und Fürstenwalde gehören. Kriminelle Hacker hätten problemlos auf die Daten zugreifen und sie sogar manipulieren können. Daten konnten eingesehen werden, die bis ins Jahr 2008 zurückreichen. Enthalten sind in etlichen Fällen sensible Patienteninformationen, die Rückschlüsse auf den Gesundheitszustand der Betroffenen ermöglichen, etwa ob der Patient im Rollstuhl sitzt, an einer Viruserkrankung leidet oder ob es sich bei der Fahrt um eine Einweisung in eine psychiatrische Klinik handelt. Hinzu kommen personenbezogene Informationen wie Namen, Adressen, Geburtsdaten und Krankenkasse der Patienten. Auch personenbezogene Daten von Teilnehmern von Erste-Hilfe-Kursen waren abrufbar. Das Einfallstor war eine Sicherheitslücke auf den Webseiten mehrerer DRK-Kreisverbände in Brandenburg.

Bereits im November 2019 hatte sich ein 18-jähriger Hacker bei einem der betroffenen DRK-Kreisverbände gemeldet. Dass die DRK-Seiten angreifbar waren, erfuhr er durch eine präzise Google-Suche. Über die Schwachstelle konnte er an Passwörter für Administratoren gelangen, die besonders weitreichende Befugnisse haben. Damit hätte er theoretisch Daten mehrerer DRK-Kreisverbände verändern können. Er wies den Kreisverband auf die Schwachstelle hin. Doch anstatt die Sicherheitslücke komplett zu beseitigen, wurde nur der Zugang zu einer der Seiten gesperrt. Da man dem Hacker nicht glauben wollte, hatte er ein Video seines Vorgehens angefertigt, gemäß dem er nach 3 Minuten die Datenbank geknackt hatte. Das Problem an sich blieb bestehen, weshalb der Hacker Kontakt zu Journalisten aufnahm. Noch bis Mitte Januar 2020 war es möglich, die Schwachstelle auszunutzen, einer sog. „SQL-Injection", bei der man sich mit unzulässigen Anfragen in das SQL-Datenbanksystem hineinschmuggelt – eine altbekannte Sicherheitslücke. Zudem hatte einer der Administratoren ein besonders leicht zu erratendes Passwort genutzt und dieses auch auf unterschiedlichen Seiten verwendet, auch solchen, die nicht mit dem DRK in Verbindung standen.

Über den Zugriff auf Server und Datenbank wäre es dem Hacker möglich gewesen, auch Krankentransporte in Echtzeit zu löschen oder zu manipulieren. So lässt sich etwa über das Setzen eines Häkchens bestimmen, dass Fahrer ohne einen Rollstuhl bei einem Patienten ankommen, auch wenn dieser eigentlich einen gebraucht hätte, so der Hacker: „Das hätte man alles live machen können."

Ob Kriminelle auf die Daten zugegriffen haben, ist unklar. Die recherchierenden Journalisten fanden Zugangsdaten des DRK-Administrators auf einer türkischsprachigen Webseite für Hacker, die bereits im Jahr 2017 veröffentlicht worden sind. Auch die besagte Schwachstelle in der Datenbankanfrage findet Erwähnung.

Das Deutsche Rote Kreuz teilt mit, man bedauere die Schwachstelle sehr. Man nehme den Vorfall „sehr ernst" und habe deutliche Konsequenzen gezogen, heißt es in einer gemeinsamen Erklärung des DRK-Generalsekretariats und des Landesverbands Brandenburg. Alle entsprechenden Webseiten seien unverzüglich abgeschaltet worden und man habe eine umfassende externe Prüfung der IT-Sicherheit veranlasst. Alle 19 Landesverbände und der Verband der Schwesternschaften des DRK seien aufgefordert worden, die Datensicherheit ihrer Webseiten und Datenbanken zu überprüfen. Auch die zuständige Landesdatenschutzbehörde sei informiert worden, ebenso das Landeskriminalamt Brandenburg. Bei der Datenschutzmeldung wurde aber bei zwei der betroffenen Kreisverbände die Meldefrist von 72 Stunden überschritten. Zunächst hatte das DRK kommuniziert, es seien „keine Details zu Diagnose oder Transportgrund" der Patienten sichtbar gewesen. Danach hieß es, man befinde sich in der Abstimmung mit dem Kreisverband, da die „geschilderten Angaben zu personenbezogenen Diagnosedaten nicht bekannt waren".

Immer wieder kommt es im Gesundheitsbereich zu Problemen mit dem Datenschutz. Den IT-Sicherheitsexperten Martin Tschirsich überrascht diese Häufung nicht. IT-Sicherheit verursache kurzfristig gesehen nur Kosten: „So kommt es, dass es in vielen Organisationen zu wenig qualifiziertes Personal und Budget dafür gibt. Zum anderen ist es dann auch oft noch so, dass jede kleine

Einrichtung sich selbst um das Thema kümmern muss, anstatt dass die Kompetenzen irgendwo gebündelt liegen“. Das mache es noch schwieriger, solche Systeme zu sichern. Auch beim Roten Kreuz organisieren Landes- und Kreisverbände ihre Webseiten und Datenbanken in eigener Verantwortung. Rechtlich seien sie „völlig selbständig“. Dennoch richtete der DRK-Landesverband Brandenburg eine E-Mail-Adresse und eine Telefonhotline ein, an die sich Betroffene wenden können (Maier-Borst/ Tanriverdi/Zierer, Zehntausende Patienten betroffen Datenleck beim Deutschen Roten Kreuz, www.tagesschau.de 05.02.2020; Müller-Hansen, Munzinger, Gekapert in drei Minuten, SZ 06.02.2020, 5).

Brandenburg

Hartge beanstandet Kfz-Kennzeichenerfassung

Nach fünf Jahren Prüfung kam die Landesdatenschutzbeauftragte von Brandenburg Dagmar Hartge zu dem Ergebnis, dass die langjährige Praxis der Polizei, mithilfe von Kfz-Kennzeichen-Scannern täglich den kompletten Autoverkehr an festen Standorten zu überwachen und die Daten zu speichern, ohne hinreichende Gesetzesgrundlage erfolgt. Der von der Polizei herangezogene § 100h Strafprozessordnung (StPO) für die automatisierte Kennzeichenerfassung sei keine Rechtsgrundlage, da überwiegend unbeteiligte Personen betroffen sind. Dass diese Daten erfasst und auf Vorrat gespeichert wurden, sei ein unzulässiger Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung.

Es gäbe weitere „gravierende datenschutzrechtliche Mängel“ beim Einsatz des Systems „Kesy“ im Aufzeichnungsmodus. Auch habe die Polizei „über den Umfang der Datenverarbeitung selbst entschieden“ und so „gegen das Gebot der Datensparsamkeit und gegen das datenschutzrechtliche Prinzip der Erforderlichkeit“ verstoßen. Die Strafverfolger sind aus Sicht der Landesbeauftragten verpflichtet zu prüfen, ob sie die über Jahre angesammelten Kennzeichendaten noch für Verfahren benötigen oder sie andernfalls löschen müssen. Es wäre auch geboten gewesen, Informationen zu den jeweiligen Ermittlungsverfahren voneinander zu trennen. Alles andere „erschwert darüber hinaus eine unverzügliche Löschung“.

Ein Rechtsgutachten im Auftrag des brandenburgischen Innenministeriums war im Juni 2019 zu entsprechenden Ergebnissen gekommen. Der zuständige Abteilungsleiter im Innenressort, Herbert Trimbach, hatte angewiesen, den Betrieb der Scanner im Aufzeichnungsmodus auszusetzen. Er wurde daraufhin versetzt, das Gutachten umgeschrieben. Der damalige Innenminister Karl-Heinz Schröter (SPD) verteidigte die Autobahnüberwachung als wichtig und unverzichtbar.

Inzwischen aktivierte die Polizei die Dauerbeschattung nur in Fällen, in denen eine hinreichend konkrete Anordnung der Staatsanwaltschaft vorlag. Auch hat sie die Zahl der Nutzungsberechtigungen reduziert. Die bereits angesammelten Kennzeichendaten blieben jedoch gespeichert. Die Sanktionsmöglichkeiten der Datenschutzaufsicht sind im Bereich Inneres und Justiz eingeschränkter als in der Wirtschaft, wo sie laut der Datenschutz-Grundverordnung hohe Bußgelder verhängen kann. Die lange Dauer ihrer Untersuchungen erklärte Hartge damit, dass sich die zu prüfende Thematik ständig weiterentwickelt und auch eine Vor-Ort-Inspektion nötig gemacht habe. Noch anhängig ist eine Beschwerde eines Autofahrers gegen Kesy vor dem Brandenburger Landesverfassungsgericht (Krempl, Datenschützerin beanstandet Kennzeichenfahndung auf Autobahnen Brandenburgs, www.heise.de 07.01.2020, Kurzlink: https://heise.de/-4629444).

Brandenburg

Kfz-Kennzeichen-Scanning wird – eingeschränkt – fortgeführt

Nach der Kritik an der Kennzeichenerfassung durch die Brandenburgische Landesdatenschutzbeauftragten rechtfertigte sich Brandenburgs Polizeipräsident Roger Höppner damit, dass sich der Datenschutz bei der massenhaften automatischen Kennzeichenfahndung auf Autobahnen deutlich verbessert habe. Die Polizei reagierte am 03.02.2020 auf Kritik der Landesdatenschutzbeauftragten Dagmar Hartge, die die bisherige Praxis als unzulässig bezeichnet hatte. In dem Schreiben von Höppner an Hartge heißt es, auf dem Server der Kennzeichenerfassung (Kesy) sollten künftig Daten jeweils nur noch maximal drei Monate gespeichert sein: „Dadurch wird der Datenumfang auf dem Kesy-Server um ein Vielfaches reduziert.“

Auf Brandenburgs Autobahnen werden seit dem Jahr 2010 wegen laufender Ermittlungsverfahren und auf Anordnung der Staatsanwaltschaften Kennzeichen erfasst und gespeichert. Als die Polizei 2019 nach der verschwundenen Rebecca aus Berlin suchte, wurde das Kesy-System bekannt. Die Datenschutzbeauftragte beanstandete diese Praxis im Januar 2020. Die Speicherung nicht mehr erforderlicher Daten sei unzulässig.

Der Polizeipräsident rechtfertigt den Aufzeichnungsmodus in seinem Schreiben grundsätzlich, will aber Mängel im Umgang mit dem Kesy-System abstellen. Er weist darauf hin, dass ohnehin nur mit Gerichtsbeschluss und per Anordnung einer Staatsanwaltschaft Daten aufgezeichnet werden. Im Januar 2020 seien bereits Daten vom 1. April 2017 bis zum 19. Juni 2019 für ein inzwischen abgeschlossenes Ermittlungsverfahren gelöscht worden. Bei diesem Ermittlungsverfahren ging es nicht nur um Brandenburg. Nach Angaben der Brandenburger Polizei ergaben 158 Anfragen an 35 Staatsanwaltschaften in 13 Bundesländern und an den Generalbundesanwalt zu Anordnungen für eine Aufzeichnung unter anderem, dass in 83 Fällen die Daten gelöscht werden sollen. In 37 Rückmeldungen gaben die Staatsanwaltschaften an, dass die Daten noch benötigt würden.

Alle Daten sollen laut Polizei nach dem Ablauf eines Beschlusses zur automatischen Kennzeichenfahndung von der Polizei gelöscht werden, aber per Datenträger an die jeweilige Staatsanwaltschaft gehen. Werden aktuell noch weiter Daten erhoben, sollen die Ermittler nach drei Monaten bei der Staatsanwaltschaft anfragen, ob diese

Daten weiter gebraucht werden oder gelöscht werden können. Derzeit haben laut Polizei 14 Sachbearbeiter des Bereichs Bandenkriminalität Zugriff zu Kesy-Daten – im vergangenen Mai seien es noch 57 gewesen. Die Datenschutzbeauftragte hatte eine fehlende Trennung der erhobenen und gespeicherten Daten für die vielen parallelen Ermittlungsverfahren kritisiert – das erschwere eine sofortige Löschung. Die Daten sollen nun nach Auskunft des Polizeipräsidenten mit Merkmalen einem konkreten Verfahren zugeordnet werden. Damit könnten auch der Standort und der Zeitraum eingegrenzt werden.

Zur Kritik der Datenschutzbeauftragten daran, dass auch die Daten nicht beschuldigter Personen erfasst werden, verwies die Polizei auf die noch laufende Verfassungsbeschwerde eines Mitglieds der Piratenpartei beim Landesverfassungsgericht. Die Frage der Pflicht einer Benachrichtigung wird laut Polizei noch rechtlich geklärt. Die Landtagsmehrheit hatte im Januar 2020 das Innenministerium dazu aufgefordert, die Beanstandungen von Hartge zu berücksichtigen und die Aufzeichnung nicht auszusetzen, so wie dies die Linksfraktion gefordert hatte. Neben der Datenerfassung zur Strafverfolgung gibt es auch die zur Gefahrenabwehr nach dem Polizeigesetz, die als unstrittig gilt.

Derweil beklagt die Landesdatenschutzbeauftragte weiter, dass die Fahnder noch immer nicht alle Rechtsverstöße abgestellt haben. Nach einer Analyse der Polizeizusagen und zwei weiteren Kontrollbesuchen vor Ort stellte sie fest, dass die Ermittler selbst nach eigenen Angaben nur Daten löschten, die sie vor dem 19. Juni 2019 erhoben haben. Einen Nachweis dafür etwa in Form eines technischen Protokolls habe die Behörde nicht vorlegen können. Zudem habe das Polizeipräsidium den kompletten, bis zum gemeldeten Stichtag angefallenen Datenbestand zuvor auf andere Speichermedien übertragen, um anfragenden Staatsanwaltschaften weiter darüber Auskunft geben zu können. So gehe der Eingriff in die Schutzrechte Betroffenen erst einmal weiter: „Ihre Daten liegen immer noch vor – neuerdings aber auf Magnetbändern und nicht mehr auf einem Server. Eine tatsächliche Löschung sieht anders aus."

Hartge bezweifelt weiterhin, dass der von den Fahndern in Anspruch genommene § 100h StPO als rechtliche Basis für den Einsatz der automatisierten Nummernschilderfassung im Aufzeichnungsmodus ausreicht. Positiv sieht Hartge nur, dass sich die Polizei an 35 Staatsanwaltschaften in 13 Bundesländern sowie an den Generalbundesanwalt gewandt habe, um den Bestand der gespeicherten Kennzeichendaten zu reduzieren. Solange noch keine Rückmeldungen über für dortige Ermittlungsverfahren noch benötigte Informationen vorlägen, bleibe der Bestand aber nach wie vor erhalten (Kennzeichenerfassung: Brandenburger Polizei sieht verbesserten Datenschutz, www.heise.de 03.02.2020, Kurzlink: https://heise.de/-4652378; Krempl, Datenschützerin: Brandenburgs Polizei trickst bei Kennzeichenfahndung, www.heise.de 13.02.2020, Kurzlink: https://heise.de/-4660497)

Hamburg

Facebook unterlässt Anzeige wegen DSB-Wechsel: Bußgeld

Die deutsche Facebook-Tochter ist vom Hamburger Datenschutzbeauftragten Johannes Caspar mit einem Bußgeld in Höhe von 51.000 Euro belegt worden, weil die Firma ihn nicht über den Wechsel ihres Datenschutzbeauftragten informiert hatte. Facebook hatte mit Anwendbarkeit der EU-Datenschutz-Grundverordnung im Mai 2018 dem Team der Hauptniederlassung in Dublin die Rolle des Datenschutzbeauftragten für alle europäischen Tochterunternehmen übertragen. Dies wurde aber nicht an die Behörde in Hamburg gemeldet, wo die Facebook Germany GmbH ihren Sitz hat. Deshalb verhängte Caspar bereits im März 2019 das Bußgeld.

Im Jahresbericht für 2019 berichtet Caspar: „Dieser Fall sollte allen anderen Unternehmen eine deutliche Warnung sein. Die Benennung des Datenschutzbeauftragten und die Mitteilung an die Aufsichtsbehörde sind Pflichten, die die DSGVO ernst nimmt." Facebook erklärte, aus Sicht des Online-Netzwerks sei es rechtlich umstritten, ob die deutsche Firma zusätzlich zur europaweit zuständigen irischen Behörde auch in Hamburg die Kontaktdaten des Datenschutzbeauftragten mitteilen müsse, so ein Sprecher: „Wir haben uns jedoch entschieden, das Bußgeld des HmbBfDI zu akzeptieren." Finanziell fällt das Bußgeld bei Facebook nicht ins Gewicht: Der Konzern hatte im jüngsten Geschäftsquartal einen Umsatz von gut 21 Milliarden Dollar (19,4 Milliarden Euro) erzielt. Der Gewinn legte auf 7,4 Milliarden Dollar (6,8 Milliarden Euro) zu (Hamburger Datenschützer verhängt Bußgeld gegen Facebook, www.heise.de 13.02.2020, Kurzlink: https://heise.de/-4660300).

Saarland

Neues Polizeirecht mit Überwachungsbefugnissen geplant

Nach Novellen in vielen anderen Bundesländern will auch die saarländische schwarz-rote Regierung das Polizeigesetz des Landes überarbeiten und Kompetenzen massiv erweitern. Der Landtag in Saarbrücken berät einen einschlägigen Entwurf. Danach sollen Ermittler mit richterlicher Erlaubnis mit technischen Mitteln in informationstechnische Systeme eingreifen, um eine Quellen-Telekommunikationsüberwachung durchführen zu können. Ziel einer solchen Maßnahme ist es, insbesondere die laufende Kommunikation über Messenger wie WhatsApp, Signal oder Threema und Internet-Telefonie via Skype & Co. direkt auf einem Zielsystem abzuhören, bevor diese ver- oder nachdem sie entschlüsselt wird. Dafür greifen Strafverfolger in der Regel auf Staatstrojaner zurück, die Sicherheitslücken ausnutzen. Eine Lizenz zu einer noch weitergehenden heimlichen Online-Durchsuchung etwa ganzer Festplatten hat die Regierung nicht vorgesehen.

Die Polizei soll „durch den Einsatz technischer Mittel auch den Standort eines mobilen Telekommunikationsendgeräts" mithilfe von IMSI- oder WLAN-Catchern feststellen dürfen. Die

bestehende Pflicht zur Bestandsdatenauskunft für Telekommunikationsfirmen will die Regierung auf sämtliche Anbieter von Telemedien und Webdiensten wie WhatsApp, Google oder Tinder erweitern. Von diesen sollen die Fahnder auch „Nutzungsdaten" wie IP-Adressen, Browsertyp, Seitenabrufe oder Besuchsdauer abfragen dürfen.

Mit Richtergenehmigung soll die Polizei ferner künftig den Aufenthalt von „Gefährdern" mit einer elektronischen Fußfessel überwachen können, wenn deren individuelles Verhalten die konkrete Wahrscheinlichkeit dafür begründet, dass sie schwere Straftaten begehen oder eine kriminelle beziehungsweise terroristische Vereinigung ins Leben rufen werden. Die Ordnungshüter müssen dabei die Annahme haben, dass die Bevölkerung auf erhebliche Weise eingeschüchtert oder die Grundstrukturen eines Staates oder einer internationalen Organisation erheblich beeinträchtigt werden sollen.

Um die neu verankerten Aufenthalts- oder Kontaktverbote durchzusetzen, sollen die Beamten das Tragen funkender Fußfesseln verordnen dürfen. Der Einsatz von Mobilfunk-Jammern zum Stören oder Unterbrechen einer Handy-Verbindung wird genauso geregelt wie der erweiterte, nun auch in Gebäuden und Wohnungen vorgesehene Bodycam-Einsatz. Die Befugnis zu Videoüberwachung öffentlicher Räume soll ausgedehnt werden auf Veranstaltungen und Ansammlungen, die generell ein „besonderes Gefährdungsrisiko" aufweisen oder von terroristischen Anschlägen bedroht sein könnten. Der Kameraeinsatz soll gemäß dem Entwurf schon möglich sein, wenn „tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden".

Weiterhin soll das umstrittene Scanning von Kfz-Nummernschildern wieder eingeführt werden. Die entsprechende „anlassbezogene automatische Kennzeichenfahndung" dürfe aber „nicht flächendeckend" erfolgen. Die Polizei soll auch eine sogenannte Referenzdatenbank mit DNA-Datensätzen eigener Mitarbeiter anlegen können, um bei einem Abgleich von Körpermerkmalen von Verdächtigen „Trugspuren" zu vermeiden.

Der Innenausschuss des Landtags hat für den 07.05.2020 eine Anhörung zu dem Entwurf angesetzt. Saarland reiht sich mit dem Vorhaben in die Phalanx anderer Bundesländer wie Bayern, Nordrhein-Westfalen, Niedersachsen und zuletzt Mecklenburg-Vorpommern ein, die trotz heftiger Proteste den polizeilichen Instrumentenkoffer massiv aufgestockt haben. Der saarländische Innenminister Klaus Bouillon (CDU) hatte zuvor mit seiner Ankündigung für Schlagzeilen gesorgt, die umstrittene Taser-Elektroschockwaffe flächendeckend allen Streifenpolizisten aushändigen zu wollen (Krempl, Saarland: Polizei soll Staatstrojaner und elektronische Fußfessel einsetzen dürfen, www.heise.de 21.03-2020, Kurzlink: https://heise.de/-4687555).

Thüringen

Datenschutzprobleme bei polizeilicher Smartphone-Ausstattung

Die Thüringer Polizisten müssen länger auf ihre dienstlichen Smartphones warten als geplant. Grund sind Datenschutzbedenken beim Verwenden von polizeilichen Anwendungen und bei der Übertragung von personenbezogenen Daten über das Internet. Die Landespolizeidirektion erklärte: „Die verfügbare Infrastruktur zum sicheren mobilen Arbeiten genügte im Ergebnis erster Betrachtungen hinsichtlich der IT-Sicherheit und damit auch des Datenschutzes den selbst gestellten Anforderungen nicht." Ursprünglich sollten Ende 2019 alle Streifenpolizisten mit einem Smartphone ausgestattet sein.

Thüringens Innenminister Georg Maier (SPD) kündigte an, dass die Digitalisierungsstrategie der Thüringer Polizei 2020 „konsequent weiter umgesetzt wird. Schwerpunkt bildet dabei in der ersten Jahreshälfte die Ausstattung des Einsatz- und Streifendienstes mit mobilen Endgeräten." Die erforderlichen Apps würden derzeit programmiert und getestet. „Hierbei ist die Gewährleistung von Datenschutz und Datensicherheit von herausragender Bedeutung."

Im Frühjahr 2019 hatten die ersten 300 Polizisten in der Polizeiinspektion Saalfeld testhalber Smartphones mit speziellen Apps für die Polizei erhalten. Die Errichtung einer sicheren Infrastruktur von mobilen Geräten und der Software habe sich aber als „aufwendiger als zunächst prognostiziert" erwiesen. „Wir wollen das nächstes Jahr so schnell wie möglich machen." Es gehe um etwa 2.000 Polizisten in Thüringen, die mit einem Smartphone ausgestattet werden sollen.

Die Thüringer Polizei führt dazu Verhandlungen mit Netzbetreibern. Die Datenschutzprobleme ergeben sich vor allem aus der Übertragung sensibler Daten per Smartphone über das Internet, so ein Sprecher: „Für die Verarbeitung der Daten durch Dritte müssen wir einen Vertrag schließen." Möglich sei etwa eine Verschlüsselung der Daten. Allerdings muss die Polizei sicherstellen, dass auch die Netzbetreiber nicht uneingeschränkt an die Daten kommen. „Ziel ist, einen Weg zu finden, wie Daten sicher übertragen werden können, ohne dass der Mobilfunkanbieter einen ungeregelten Zugriff darauf hat." Bei Laptops, die im Außeneinsatz genutzt werden, sei die Verschlüsselung mithilfe eines externen Gerätes gelöst. Für Smartphones sei diese Lösung aber nicht geeignet, weil sie dadurch unhandlich würden.

Mit den Smartphones sollen Polizisten nach den Vorstellungen der Thüringer Polizei in Zukunft einfache Sachverhalte bereits von unterwegs in das polizeiliche Verarbeitungssystem einspeisen können. Außerdem soll es möglich sein, zum Beispiel Ausweisdokumente direkt mit dem Smartphone auszulesen und per Internetverbindung überprüfen zu lassen. Dabei sollen die Beamten unter anderem die Echtheit der Dokumente prüfen und Informationen erhalten können – zum Beispiel ob gegen die überprüfte Person eine Fahndung läuft. Auch eine Foto-App sollen die Beamten auf ihren Smartphones nutzen können. Damit sollen etwa Auto-Kennzeichen abfotografiert und überprüft werden können (Digitalisierung der Thüringer Polizei verzögert sich, www.heise.de 23.12.2019. Kurzlink: https://heise.de/-4622011).

Datenschutznachrichten aus dem Ausland

Weltweit

„Operation Rubikon“: Staatsverschlüsselung für BND und CIA

Der Bundesnachrichtendienst (BND) und der US-Auslandsgeheimdienst CIA haben mittels der Verschlüsselungsfirma Crypto AG mit Sitz in dem Schweizer Städtchen Steinhausen über Jahrzehnte hinweg mehr als 100 Staaten ausgespäht. Medienberichten zufolge, die auf die Auswertung von bisher unveröffentlichten CIA- und BND-Dokumenten über die von 1970 bis 1993 laufende „Operation Rubikon“ zurückgehen, verließen sich Regierungen in aller Welt bei der Verschlüsselung ihrer Kommunikation auf die Firma im Unwissen darüber, dass diese seit 1970 in Besitz der CIA und des BND war und die Geheimdienste so in der Lage waren, die Verschlüsselung zu knacken.

Das Unternehmen produzierte zwei Arten von Geräten: wirklich abhörsichere und solche, die von den Diensten geknackt werden konnten. Bei den fehlerhaften Geräten war die Verschlüsselung bewusst weniger kompliziert: Wer die Technik kannte, konnte mitlesen. Ein Modell wurde gar komplett von der NSA entworfen. Regierungen und Militärs, die die Geräte kauften, vertrauten auf die vermeintlich sichere Technik aus der neutralen Schweiz. Tatsächlich hörten USA und BND mit.

Der frühere Kanzleramtsminister Bernd Schmidbauer bestätigte die „Operation Rubikon“ und meinte: „Die Aktion Rubikon hat sicher dazu beigetragen, dass die Welt ein Stück sicherer geblieben ist.“ Der BND habe die Zusammenarbeit mit der CIA demnach aber 1993 beendet. Die Crypto AG war seit Ende des Zweiten Weltkriegs bis zum Beginn dieses Jahrhunderts einer der größten Anbieter für abhörsichere Kommunikation und verkaufte diese weltweit. Zu den Kunden zählten rund 120 Länder, darunter der Iran, südamerikanische Regierungen sowie Indien, Pakistan und der Vatikan. BND und CIA waren demnach ab 1970 jeweils zur Hälfte Eigentümer der Firma. Die Kunden hätten nicht gewusst, dass BND und CIA die Technik manipulieren ließen.

Die größten Abnehmer für die manipulierte Technik waren demnach Saudi-Arabien und der Iran. Jahrzehntelang seien deutsche und US-Stellen über die geheime Regierungskommunikation des Iran informiert gewesen, auch während der Geiselnahme in der US-Botschaft in Teheran 1979. Die Dokumente belegten außerdem erstmals, dass BND und CIA frühzeitig über den Sturz des chilenischen Präsidenten Salvador Allende 1973 und schwere Menschenrechtsverletzungen durch die argentinische Militär-Junta informiert waren, bei denen Tausende Regimegegner verschwanden und zum Beispiel aus Hubschraubern lebendig ins Meer geworfen worden waren.

Den Berichten zufolge haben CIA und BND Millionen Euro an der Firma verdient, so ein Zitat aus den ausgewerteten Papieren: „Die jährliche Gewinnausschüttung (…) wurde dem BND-Haushalt zugeschlagen, (…) Haushaltsausschuss und Rechnungshof hatten darüber keine Kontrolle.“ So wurden die Staaten Dank ihrer Leichtgläubigkeit nicht nur ihrer Geheimnisse, sondern auch ihres Geldes beraubt. Das Schweizer Verteidigungsministerium teilte mit: „Die zur Diskussion stehenden Ereignisse nahmen um 1945 ihren Anfang und sind heute schwierig zu rekonstruieren und zu interpretieren.“

Der „Spiegel“ hatte die Crypto AG in einem Artikel 1996 die „allererste Adresse bei den Heimlichkeitswerkzeugen“ genannt und über „verworrene“ Besitzverhältnisse berichtet und dass deutsche und amerikanische Geheimdienste im Verdacht stünden, „bis Ende der achtziger Jahre Cryptos Schutzgeräte so manipuliert zu haben, dass ihre Codes im Handumdrehen zu knacken waren“. Er vermutete „die dreisteste Geheimdienstfinte des Jahrhunderts“.

In der Schweiz lösen die Enthüllungen Bestürzung aus. Gemäß den Recherchen waren die schweizerischen Geheimdienste über Jahrzehnte eingeweiht; es liegen Hinweise vor, nach denen sogar „Schlüsselpersonen in der Regierung“ von der Operation wussten. Nun fürchten viele um den Ruf ihres Landes. Als neutraler Staat genießt die Schweiz besonderes Vertrauen, weshalb sie häufig als Vermittlerin bei Konflikten auftritt oder als „Briefträgerin“ zwischen Staaten fungiert, die ihre Beziehungen abgebrochen haben. Der Bundesrat, die Schweizer Regierung, erfuhr aufgrund von Mediennachfragen schon im November 2019 von der Recherche und entzog den Nachfolgefirmen der Crypto AG die Ausfuhrbewilligung. Die Crypto AG soll 2018 in zwei Firmen aufgespalten worden sein. Den neuen Geschäftsleitungen lägen, so Medienberichte, über die Zeit davor keine Erkenntnisse vor. Der Schweizer Bundesrat hat am 15.01.2020 Niklaus Oberholzer, bis Ende 2019 Bundesrichter, damit beauftragt, die Faktenlage zu klären. Bis Ende Juni soll sein Bericht vorliegen.

Schweizer Parlamentarier fordern nun die Einsetzung einer Parlamentarischen Untersuchungskommission (PUK), des mächtigsten Kontrollinstruments, das dem Parlament zur Verfügung steht. Im Februar kündigten die Sozialdemokraten bereits an, im Frühling eine entsprechende Initiative einzureichen. Es wäre erst die fünfte PUK in der Geschichte der Schweiz. Offen für eine Einsetzung zeigten sich auch Vertreter der Grünen und der FDP; auch die Schweizerische Volkspartei (SVP) zieht in Betracht, zuzustimmen. Über mögliche Verbindungen der Crypto AG zu Geheimdiensten wurde schon seit den Neunzigerjahren berichtet. Die nun in Auszügen veröffentlichten Berichte der Dienste kommen aber Geständnissen gleich und enthüllen, wie eiskalt BND und CIA ihr Geschäft betrieben. Über die Crypto-Maschinen spionierte der deutsche Dienst sogar Verbündete aus - darunter die Nato-Mitglieder Spanien, Italien, Portugal und die Türkei.

Nur wenige hochrangige Crypto-Mitarbeiter waren in das doppelte Spiel eingeweiht. Sie waren Helfer der Ge-

heimdienste, ohne genau zu wissen, wer die Fäden zog. 1992 dann die Krise: Iran verhaftete den Crypto-Vertreter Hans Bühler und warf ihm Spionage vor. Er wusste nicht, dass er mit Ware handelte, die manipuliert worden war. Der BND kaufte ihn für eine Million Dollar frei. Auch weil Bühler später selbst den Verdacht äußerte, die Geräte seiner Firma seien womöglich Spionagewerkzeuge, wurde es der Bundesregierung zu heiß. Sie stieg 1993 aus dem Projekt aus. Laut den jüngsten Enthüllungen betrieb die CIA die Operation noch bis 2018 weiter. Danach spaltete sich die Firma auf und ging an neue Eigentümer.

Der deutsche Bundestagsabgeordnete Konstantin von Notz (Grüne) forderte die Bundesregierung auf, im Parlamentarischen Kontrollgremium (PKGr) Stellung zu nehmen. Er ist stellvertretender Vorsitzender des PKGr, über das der Bundestag die Geheimdienste kontrollieren soll. Es sei zu klären, „ob die parlamentarische Kontrolle vorsätzlich über rund zwei Jahrzehnte umgangen wurde". Stephan Thomae, der für die FDP im PKGr sitzt, hat vor allem eine Frage an die Bundesregierung: „Es gab Gewinne, die offenbar in einen Schattenhaushalt des BND geflossen sind. Wo sind diese Gelder verblieben?" Eine Sprecherin der Bundesregierung sagte lediglich, man habe die Berichte „zur Kenntnis genommen". Der BND selbst erklärte: „Der Bundesnachrichtendienst nimmt zu Angelegenheiten, welche die operative Arbeit betreffen, grundsätzlich nicht öffentlich Stellung" (Geheimdienste CIA und BND hörten gemeinsam ab, www.tagesschau.de 11.02.2020; BND und CIA spähten mittels gemeinsamer Firma Staaten aus, www.tagesspiegel.de 11.02.2010; Brühl/Pfaff, Von wegen neutral, SZ 13.02.2020, 6).

Weltweit

Millionen Facebook-Nutzerdaten offen im Netz

Sicherheitsforscher haben eine ungesicherte Datenbank mit offenbar gestohlenen Informationen von 267 Millionen Facebook-Nutzern im Netz entdeckt. Die Datenbank mit Basisinformationen befand sich rund zwei Wochen lang auf einem ungesicherten Server im Internet. Die Datensätze bestanden offenbar aus Namen, Telefonnummer und zugehöriger User-ID. Wie die britische Tech-Webseite „Comparitech" in Zusammenarbeit mit dem Sicherheitsforscher Bob Diachenko berichtet, waren sie Mitte Dezember 2019 auf eine Elasticsearch-Datenbank mit den Daten gestoßen, die seit dem 04.12.2019 ohne Passwortschutz im Netz stand. Am 19.12. sei der Server allerdings offline gegangen.

Bei dem Datensatz handelte es sich um Informationen, die mutmaßlich mit kriminellen Absichten gesammelt wurden. Die Daten stammen möglicherweise aus Facebooks Entwickler-API und waren abgegriffen worden, bevor Facebook die Suche nach Telefonnummern im April 2018 im Zuge des Cambridge-Analytica-Skandals abgeschaltet hatte. Bis dahin war es möglich gewesen, durch massenhaftes Abgleichen von existierenden Telefonnummern die zugehörigen Facebook-Profile zu ermitteln. Die Informationen wären demnach knapp zwei Jahre alt. Eine alternative Methode hätte im automatischen Durchforsten öffentlicher Facebook-Profilinformationen bestanden.

Die betroffenen User stammen laut dem Bericht überwiegend aus den USA, wobei Spracheinstellungen des Datenbankservers auf vietnamesische Datensammler hindeuten. Besonders die enthaltenen Telefonnummern sind problematisch, da sie für SIM-Swapping oder Phishingversuche per SMS benutzt werden könnten. Facebook bestätigte den Vorgang. Man vermute, dass die Daten tatsächlich vor den Beschränkungen der Suchmöglichkeiten gesammelt worden seien. Eine ähnliche, offen einsehbare Datenbank mit mehr als 410 Mio. Betroffenen aus den USA, Großbritannien und Vietnam war im September 2019 von „TechCrunch" entdeckt worden. In der damaligen Sammlung waren ebenfalls User-ID und Telefonnummern, aber auch Namen und teils Geschlecht und Staatsangehörigkeit enthalten (Koenigsdorff, Daten von 267 Millionen Facebook-Nutzern offen im Netz, www.heise.de 20.12.2019, Kurzlink: https://heise.de/-4621213).

Europa

Datenschutzbeauftragte fordern EU-Datenschutzbehörde im privaten Bereich

Deutsche Datenschutzbeauftragte fordern für internationale Konzerne die Einrichtung einer europaweit zuständigen zentralen Datenschutzbehörde. Die schleswig-holsteinische Datenschutzbeauftragte Marit Hansen erklärte, es habe sich nicht bewährt, dass allein die irische Behörde bei großen internationalen Konzernen wie Facebook zuständig sei. Eine unabhängige Einrichtung könne frei entscheiden, unabhängig davon, wo ein Konzern seine Steuern zahle. Bei einer EU-Behörde müsse man „keine direkte oder indirekte politische Einflussnahme aus den Mitgliedstaaten befürchten". Auch der Hamburger Datenschutzbeauftragte Johannes Caspar kritisiert das aktuell in der DSGVO geregelte Verfahren als „schwerfällig, überbürokratisch und ineffizient". Es räume der federführenden Behörde zu viele Rechte ein und ermögliche ihr, den Entscheidungsfluss völlig zum Erliegen zu bringen. Änderungen seien nötig, „um Rechte und Freiheiten Betroffener gerade gegenüber globalen Diensteanbietern durchzusetzen, aber auch um einen fairen Wettbewerb auf dem digitalen Binnenmarkt sicherzustellen" (Gries, Deutsche Datenschutzbeauftragte fordern europäische Datenschutz-Behörde, https://www.turi2.de 25.02.2020).

Europa

Buchungsplattformen werden statistisch erfasst

Buchungen über Airbnb, Booking, Expedia und Tripadvisor sollen erstmals europaweit statistisch erfasst werden, um einen Überblick über die in manchen Städten beklagten Auswüchse der privaten Zimmervermittlungen zu erhalten. Die EU-Kommission teilte am 05.03.2020 mit, dass hierbei Nutzende nicht registriert und der Datenschutz gewahrt würden. Nach Angaben der Brüsseler Behörde haben die vier Vermittlungsportale eine Vereinbarung mit

dem EU-Statistikamt Eurostat getroffen. Geliefert würden Zahlen zu gebuchten Übernachtungen und Gästen, so EU-Wirtschaftskommissar Paolo Gentiloni: „Künftig können Behörden diese neu verfügbaren Daten für eine fundierte Politikgestaltung nutzen."

Die Plattformen für private Unterkünfte stehen in der Kritik. Den Betreibern wird vorgeworfen, die Wohnungsnot zu verschlimmern, weil Wohnungen als Ferienwohnungen zweckentfremdet würden. Der für den Binnenmarkt zuständige EU-Kommissar Thierry Breton sagte, die Vermietung privater Unterkünfte sei bequem für Touristen und eine Einnahmequelle für Besitzer. Die Kommission stehe dem positiv gegenüber: „Gleichzeitig wird sie die lokalen Gemeinschaften dabei unterstützen, die Herausforderungen zu bewältigen, die sich aus diesem raschen Wandel ergeben" (Airbnb und Co. liefern Eurostat Daten, www.wienerzeitung.at 05.03.2020).

Europa

Facebook verbreitet Nebelkerzen gegen Internet-Regulierung

Nick Clegg, der früher stellvertretender britischer Premierminister war, ist jetzt als Facebooks „Außenminister" für die globale Beziehungspflege des Internetkonzerns zuständig. Im September 2019 appellierte er auf einer Facebook-Veranstaltung dafür, Scharmützel über den Zugang zu Daten oder kartellrechtliche Schritte zu lassen und sich dem „Kampf um die Seele des Internets" zu stellen. Die Gräben verliefen dabei nicht etwa zwischen Europa und den USA, sondern zwischen dem Westen und der wachsenden Zahl an Ländern vor allem in autoritär regierten Ländern, die das Konzept einer „chinesischen Mauer" im Netz übernehmen wollten. Europa und die USA müssten gemeinsam gegen diese neuen chinesischen Mauern im Netz kämpfen.

Facebook selbst habe als US-amerikanisches Unternehmen „viel mit den europäischen Werten" gemein, erklärte Clegg im Zusammenhang mit einem Gespräch mit den EU-Kommissaren Věra Jourová und Valdis Dombrovskis, die die Ressorts „Werte und Transparenz" sowie „Wirtschaft und Kapitaldienstleistungen" leiten. Akteure in Europa und den USA seien bemüht, ein „offenes, freies und grenzenloses Internet zu schützen". Dem gegenüber stehe China, das auf ein staatlich überwachtes und eingeschränktes Netz setze.

Die politischen Entscheidungsträger müssten laut Clegg „den Einfallsreichtum und die Freiheit schützen", die das Internet bisher im Westen ausmachten. Facebook erhoffe sich gerade von der EU-Kommission neue Gesetze und Vorgaben nach diesen Prinzipien. Zuvor hatte Facebook-Chef Mark Zuckerberg bereits von der Politik weltweit einheitliche Regeln für den Umgang mit gefährlichen Inhalten oder zum Datenschutz verlangt, bei denen aber auch die Meinungsfreiheit berücksichtigt werden sollte.

Die neue Kommission unter Ursula von der Leyen (CDU) will unter anderem den Entwurf für einen „Digital Services Act" vorlegen, mit dem Online-Plattformen stärker in die Verantwortung genommen werden sollen. Für Konzerne wie Facebook sind Clegg zufolge Grundregeln erforderlich, damit sie nicht länger als „Online-Schiedsrichter" in politischen Auseinandersetzungen fungieren müssten. Dem Beispiel von Twitter, politische Werbung zu untersagen, werde Facebook aber nicht folgen. Bei solchen Kampagnen handle es sich um eine „legitime Nutzung unserer Plattform". Skeptisch äußerte sich Clegg zum Drängen der Kommission, Datensätze offenzulegen, die das Unternehmen über seine Nutzer speichert. Ein weitergehender Ansatz zum Teilen von Daten mit Wettbewerbern im Sinne etwa einer Interoperabilität von Messenger-Diensten könne auch ein Risiko für die Privatsphäre der Betroffenen bedeuten (Krempl, EU-Regulierung: Facebook will für die „Seele des Internets" streiten, www.heise.de 06.12.2019, Kurzlink: https://heise.de/-4607057).

Niederlande

System gegen Sozial- und Steuerbetrug wegen Datenschutzmängeln gestoppt

Die Niederlande stoppen den Einsatz eines Computersystems gegen Sozial- und Steuerbetrug, nachdem ein Gericht das Verknüpfen gespeicherter Einwohnerdaten für unrechtmäßig erklärt hat. Das Sozialministerium in Den Haag teilte am 05.02.2020 mit, dass die Privatsphäre der Bevölkerung laut dem Urteil unzureichend geschützt sei, weshalb das Computersystem außer Betrieb genommen werde. Das zunächst nur in einigen Städten eingesetzte Computersystem konnte zu einer Person vielfältige Daten verknüpfen, etwa zum Arbeitsleben, zu Steuern, Schulden, Immobilienbesitz, Einbürgerung, Ausbildung, Sozialleistungen oder auch zu beantragten Genehmigungen für bestimmte berufliche Aktivitäten. Das Gericht in Den Haag hatte den Behörden in seinem Urteil vom gleichen Tag zwar grundsätzlich das Recht eingeräumt, im Kampf gegen Sozialbetrug neue technologische Möglichkeiten zu nutzen. Allerdings müsse es einen transparenten Schutz der Daten der Bürger geben. Dem werde das eingesetzte Computersystem SyRI nicht gerecht (Niederlande stoppen Einsatz von Computerprogramm gegen Sozialbetrug, www.greenpeace-magazin.de 05.02.2020).

Israel

Wählerdaten im Netz frei verfügbar

In Israel hat die rechtsnationale Partei von Premier Benjamin Netanjahu personenbezogene Daten von rund 6,5 Millionen Bürgerinnen und Bürgern in eine App geladen, sodass sie tagelang im Internet frei zugänglich waren. Laut Medienberichten waren Namen, Personalausweisnummern, Adressen sowie Telefonnummern aller Israelis über 18 Jahre abrufbar. Bei rund 600.000 Personen hatten Parteimitarbeiter hinzugefügt, dass diese Person den Likud nicht unterstütze. Die Partei bestätigte die Sicherheitslücke und machte den Anbieter der App dafür verantwortlich, die israelische Firma Feed-b. Wie in anderen Ländern auch bekommen in Israel Parteien vor Wahlen Zugang zum Wählerregister und sind dann dafür verantwortlich, dass der Datenschutz gewährleistet bleibt. Es war schon das zweite Mal, dass Likud Fahrlässigkeit im Umgang

mit personenbezogenen Informationen vorgeworfen werden musste (Föderl-Schmid, Gefährlich sorglos, Datenpanne beim Likud, SZ 12.02.2020, 4, 6).

USA/Deutschland

Nutzung von Clearviews Gesichtsdatenbank durch Private und Behörden

Über das Unternehmen Clearview mit seiner globalen Gesichtsdatenbank (DANA 1/2020, 68 f.) wurden weitere Erkenntnisse öffentlich. Die Datenbank enthält angeblich drei Milliarden Bilder und begleitende Informationen, die Clearview aus sozialen Netzwerken und vielen anderen Websites zusammenkopiert hat, ohne dabei irgendjemanden um Erlaubnis zu bitten. Nach dessen eigenen Angaben ist die umstrittene Gesichtserkennungs-App ein „Recherche-Werkzeug für Strafverfolger, um Täter und Opfer von Verbrechen zu identifizieren". Doch berichten Medien, dass auch zahlreiche Bildungseinrichtungen, Unternehmen und Privatdetekteien auf der Kundenliste stehen. Außerdem wurde sie lange Zeit auch von Investoren und Freunden der Gründer zu privaten Zwecken benutzt. Nach der kritischen Berichterstattung über das Unternehmen und sein Produkt veröffentlichte Clearview AI einen Verhaltenskodex, wonach die App „nur für Strafverfolger und ausgesuchte Sicherheitsexperten zugänglich" sei. Sie enthalte „Sicherheitsvorkehrungen, damit diese Profis sie nur für den beabsichtigten Zweck nutzen".

Wer früh in das Start-up investierte, bekam aber nach den Presseberichten einen privaten Zugang zur App als Anreiz. Mitgründer Hoan Ton-That bestätigte diese Testzugänge für die sorgfältige Prüfung der Technik durch potenzielle Investoren und „strategische Partner". So verwendete etwa der Milliardär John Catsimatidis die Software, um den ihm unbekannten Begleiter seiner Tochter in einem Restaurant zu identifizieren. Er bat dazu den Kellner, den Mann zu fotografieren. Das Foto lud er dann in die App, für die er einen Nutzeraccount hatte, und glich es so erfolgreich mit Clearviews riesiger Datenbank ab. Die App verriet ihm, dass es sich beim Freund seiner Tochter um einen Risikoinvestor aus San Francisco handelte. Später wurde die Technik von seiner Supermarktkette eingesetzt, um Ladendiebe wiederzuerkennen. Catsimatidis sah es als „großes Problem" an, dass jemand Häagen-Dasz-Eiscreme klaute.

Gemäß einem anderen Investor sollen dessen beiden schulpflichtigen Töchter sich einen Spaß gemacht haben, mit der App zu spielen und sie an sich selbst und Freunden auszuprobieren, um zu erfahren, wem sie ähnlich sehen. Weitere Personen mit Clearview-Zugängen haben die App demnach bei Dates und Geschäftsveranstaltungen verwendet. In den Händen von Privatpersonen kann solch eine App zum Stalking verwendet werden. In der Öffentlichkeit wäre niemand, von dem es im Internet frei zugängliche Fotos gibt, noch vor einer unfreiwilligen und heimlichen Identifizierung geschützt.

Auf seiner Website bietet Clearview AI für EU-Bürgerinnen und –Bürger ein Formular, mit dem diese beantragen können, aus der Datenbank gelöscht zu werden. Wer das erreichen will, muss allerdings ein Foto von sich hochladen und sich identifizieren.

In Deutschland überprüft der Hamburgische Datenschutzbeauftragte (HmbBfDI) Johannes Caspar auf eine Beschwerde hin die auf automatisierte Gesichtserkennung spezialisierte Firma Clearview AI. Auskünfte, die ein betroffener Beschwerdeführer von dem Unternehmen erhalten habe, „geben Anlass zu einer Reihe von Fragen über das dahinterliegende Datenverarbeitungsmodell". Ein Sprecher des HmbBfDI: „Mit anderen europäischen Aufsichtsbehörden, die ähnliche Untersuchungen durchführen, werden wir uns abstimmen." Parallel gelte es zu klären, welche Unternehmen oder Sicherheitsbehörden in Deutschland Kunden von Clearview sind beziehungsweise waren. Sollten sich Berichte bestätigen, dass europäische Polizeiämter die „fragwürdigen Angebote" der Firma genutzt hätten, „wäre dafür zu sorgen, dass dies umgehend abgestellt" und für die Zukunft ausgeschlossen wird.

Der Bundesdatenschutzbeauftragte Ulrich Kelber stellte klar, dass er etwa für das Bundeskriminalamt (BKA) für den Einsatz einer solchen Technik „keine gesetzliche Grundlage" sieht. Gemäß dem HmbBfDI besteht „Grund zu der Annahme, dass die Verarbeitung biometrischer Daten von Millionen von Nutzern auf keiner tragfähigen rechtlichen Grundlage beruht". Das Vorgehen der Firma verstoße damit gegen Vorgaben der Datenschutz-Grundverordnung (DSGVO). Gleiches gelte „für diejenigen verantwortlichen Stellen, die das Angebot von Clearview nutzten, da sie einen Teil der datenschutzrechtlichen Verantwortung tragen".

Sollten Bürger Anhaltspunkte dafür haben, dass ihre Daten von Clearview verwendet würden, steht ihnen ein Auskunftsrecht zu. Dieses können sie direkt bei dem Unternehmen geltend machen, um zu erfahren, ob sie tatsächlich betroffen sind und gegebenenfalls etwa auch eine Löschung beantragen. Die von Clearview geforderten Ausweisdokumente sollten dabei aber nur in um nicht erforderliche Daten geschwärzter Form übersendet werden. Dass die Firma eine Ausweiskopie verlangt, hält Caspar für problematisch. Dem Unternehmen würden so „zusätzliche Daten zugespielt". Unabhängig davon sei bereits gesetzlich geregelt, dass unrechtmäßig beschaffte und verarbeitete Informationen zu löschen sind. Es bedürfe dazu keines individuellen Antrags. Dies zu klären und gegebenenfalls durchzusetzen, sei Aufgabe der Aufsichtsbehörden: „Wir werden diese rechtlichen Anforderungen nach Maßgabe unserer Prüfung geltend machen."

Der Fall zeigt für Caspar, „dass die Technologie der Gesichtserkennung massive Risiken für die Privatsphäre mit sich bringt und kaum zu kontrollieren ist". Die Sicherheitsbehörden sollten ihre eigenen Überlegungen zur Nutzung biometrischer Werkzeuge daher auf den Prüfstand stellen. Sie bräuchten dafür eine klare rechtliche Basis, aus der sich „insbesondere Anlass, Ort und Zeit der Maßnahme, Informations- und Auskunftspflichten sowie ein Richtervorbehalt für die Anordnung ergeben". Clearview konnte laut Caspar offenbar eine große Datenbasis aufbauen, „da es sich aus öffentlich zugänglichen Daten" wie Profilbildern der Nutzer von Facebook & Co. bedient habe. Die Betreiber hätten es daher wohl versäumt, „ein solches

massenhaftes Scraping der Daten effektiv zu verhindern". Anbieter sollten verstärkt in die Pflicht genommen werden, um durch technische Maßnahmen im Einklang mit dem Grundsatz „Privacy by Design" ein solches Vorgehen von vornherein zu verhindern (Krempl, Gesichtserkennung: Hamburgischer Datenschützer geht gegen Clearview vor, www.heise.de 10.03.2020, Kurzlink: https://heise.de/-4687290; Clearviews Gesichtserkennung wurde auch privat genutzt, www.spiegel.de 05.03.2020).

USA

Schlechtes Zeugnis für Predictive Policing in LA

Die Polizei in Los Angeles (LA) verfolgte mit dem Überwachungsprogramm „Operation LASER" das Ziel Verbrechen zu verhindern, bevor sie geschehen. Dies wurde nicht erreicht, wohl aber produzierte das Verfahren systematisch Diskriminierung. Die Polizei wollte Schwerkriminelle und Gangmitglieder „wie Tumore" im Blick behalten. Mithilfe von „Operation LASER" sollten sie mit „laser-ähnlicher Präzision" aus gewaltgeplagten Vierteln entfernt werden, so eine Projektbeschreibung. Die übrigen Bewohner sollten möglichst unbeschadet bleiben. Mitte Dezember 2019 gelangten Informationen an die Öffentlichkeit, wonach fast ausschließlich Latinos und Schwarze überwacht wurden. Aufstieg und Fall von „Operation LASER" werfen ein Schlaglicht auf die generell mit „Predictive Policing" verbundenen Probleme. Dabei soll mit datengestützten Prognosen die Wahrscheinlichkeit zukünftiger Verbrechen an bestimmten Orten oder die potenzielle Gefährlichkeit von Personen berechnet werden.

Die Bürgerrechtsorganisation „Stop LAPD Spying Coalition" hatte nach einer Klage gegen die Polizei von Los Angeles Dokumente erhalten, die eine rassistische Verzerrung belegen, darunter eine Liste mit 679 Zielpersonen. Die Bewertung von Hamid Khan, dem Gründer der Organisation: „Die Daten zeigen, dass 89 Prozent der überwachten Personen People of Color, also nicht weiß sind." Mit insgesamt 44 Prozent schwarzen Zielpersonen sei der Fokus auf die schwarze Bevölkerung „überwältigend": „Die schwarze Gemeinschaft hat in Los Angeles nur einen Anteil von rund neun Prozent an der Gesamtbevölkerung, also ist es eine Verzerrung von 5:1."

Prognosesoftware soll theoretisch objektivere Einschätzungen liefern als Polizeibeamte aus Fleisch und Blut und eine gezieltere und kostensparende Polizeiarbeit ermöglichen. An der Zuverlässigkeit der Vorhersagen bestehen jedoch Zweifel, unabhängige Erfolgsbeweise existieren nicht. Dennoch hat sich Predictive Policing weltweit – auch in Deutschland – ausgebreitet. Sicherheitsbehörden versuchen hierzulande etwa mit RADAR-iTE die Gefährlichkeit von Terrorverdächtigen zu berechnen. Ein halbes Dutzend Landeskriminalämter setzt zudem auf Einbruchsvorhersagen.

In einer Studie der Stiftung Neue Verantwortung und der Bertelsmann Stiftung zum Predictive Policing warnt Tobias Knobloch: „Wie gut das Einkreisen von Kriminalitäts-Hotspots funktioniert, weiß man nicht, weil die Wirkung sehr schwer messbar ist." Jeder Erfolg sei spekulativ, weil er im Ausbleiben von Kriminalität bestehe. „Andere mögliche Einflussfaktoren" ließen sich nicht so isolieren, „dass man Wirkungen unmittelbar auf Predictive Policing zurückführen" könne. Auch Prognosen zur Gefährlichkeit oder zum Rückfallrisiko von Straftätern oder Verdächtigen sind umstritten.

In amerikanischen Metropolen wie Los Angeles und Chicago untersuchen mittlerweile polizeiliche Aufsichtskommissionen die Programme, was Hamid Khan grundsätzlich begrüßt: „Operation LASER wurde lange eingesetzt, ohne dass außerhalb der Polizei irgendjemand wusste, was da abläuft und ohne zu verstehen, dass gerade ein Paradigmenwechsel zu datenbasierter Polizeiarbeit stattfindet.". Von einem Gemeinschaftszentrum in der Skid Row aus, jenem Stadtviertel von Los Angeles, in dem Tausende Obdachlose auf der Straße leben und ständig Polizeikontrollen stattfinden, erforscht Khan seit 2010 mit einem Team von Freiwilligen und Betroffenen den Überwachungsapparat des LA Police Department (LAPD), wobei er auf „Operation LASER" stieß.

Mit Fördermitteln aus der „Smart Policing Initiative" des US-Justizministeriums hatten das LAPD und die private IT-Firma Justice & Security Strategies 2009 begonnen, zu analysieren, in welchen Stadtgebieten in den Vorjahren die meisten Schießereien und Vorfälle mit Waffengewalt gemeldet wurden. Dabei wurden Hotspots mit hohen Kriminalitätsraten und „Anchor Points" wie Shopping-Malls, Parks, Obdachlosenunterkünfte oder Alkohol-Geschäfte identifiziert. Im September 2011 lief „Operation LASER" zunächst in der Newton Division an und wurde dann nach und nach auf weitere Stadtviertel ausgedehnt.

Im Rahmen des „Chronic Offender Program" erstellte die Polizei zudem für jedes Gebiet ein Ranking mit mindestens zwölf Serientätern, auf die sich die Polizeiarbeit konzentrieren sollte. Für das Scoring wurden Punkte nach Kriterien wie Gangmitgliedschaft, Gewalttaten in der Vergangenheit, Verhaftungen, Bewährungsstrafen oder kürzliche „Polizeikontakte" addiert. In die Erstellung von personenbezogenen Profilen flossen zudem Analysen mit Software der umstrittenen Firma Palantir ein, die auch in Europa, etwa bei der Landespolizei von Hessen, zum Einsatz kommt und die verschiedene Polizeidatenbanken scannt.

Der Fokus auf kleine Gruppen von Schwerkriminellen sollte auch das Rambo-Image der LAPD vergessen machen, das lange als Amerikas brutalster und rassistischster Polizeiapparat galt. Die LAPD war mit dem Rampart-Skandal oder mit Massenverhaftungen im Zuge der „Operation Hammer" aufgefallen. Die Polizei stehe mittlerweile unter Rechtfertigungsdruck, so Hamid Khan: „Es ist eine Evolution, dass das LAPD jetzt sagt: ‚Wir wollen nicht die ganze Community stören, sondern wir kommen, um die Schlimmsten der Schlimmen zu holen.'" Für ihn ist Predictive Policing dennoch kein echter Wandel hin zu einer faireren Polizeiarbeit, sondern „eine pseudowissenschaftliche Maskerade für die Kriminalisierung und Überwachung gesellschaftlicher Minderheiten – eine Art Formel, mit der die Polizei der Öffentlichkeit gegenüber begründen kann, warum sie tut, was sie tut".

Nach viel öffentlicher Kritik hat auch die Polizeikommission „Operation LASER" inzwischen eine vernichtende Bilanz ausgestellt. Sie warnt davor, Schlüsse aus den Daten zum angebli-

chen Erfolg des Programms zu ziehen. Die Daten weisen zahlreiche Widersprüche auf, auch die Präsenz der Polizei in den Schwerpunktgebieten war offenbar begrenzt. Der Kommission zufolge wurde ein Großteil der per GPS automatisch erfassten Anwesenheitszeiten der Polizei in den „Hotspots" durch geparkte Autos erzeugt oder durch Polizisten, die an dem Ort vorbeifuhren.

Zudem prangert die Kommission in ihrem Ende März 2019 veröffentlichten Untersuchungsbericht gravierende Inkonsistenzen bei der Verwaltung des „Chronic Offender Program" an, „insbesondere in Bezug auf die Auswahl- und Dokumentationspraktiken von Gebiet zu Gebiet": „Diese Unterschiede scheinen auf einen Mangel an zentralisierter Aufsicht sowie auf einen Mangel an formalisierten und detaillierten Protokollen und Verfahren zurückzuführen zu sein." Die meisten als „Wiederholungstäter" kategorisierten Personen hätten wenige oder keine Polizeikontakte gehabt. Einige der Zielpersonen seien zwar kontrolliert oder verhaftet worden; dies sei aber nicht klar auf „Operation LASER" zurückzuführen.

Allein Kriterien wie Gangmitgliedschaft, die in Predictive Policing einfließen, offenbaren, wie problematisch die Einstufung von Kriminellen ist. US-Gang-Datenbanken sind oft fehlerhaft und veraltet. Menschen werden kriminalisiert, ohne jemals verhaftet worden zu sein. Afroamerikaner und Latinos sind überproportional vertreten. Ein Prüfbericht von 2016 offenbarte, dass Kaliforniens Gangdatenbank „CalGang System" zahlreiche Fehler enthielt. Babys waren darin registriert, die angeblich zugegeben hatten, Gangmitglieder zu sein.

Technologien wie Predictive Policing verschleiern Ruha Benjamin, Professorin von der Princeton University, zufolge Rassismus: „Algorithmen schaffen ein Hightech-Alibi für das routinemäßige Racial Profiling, Schikanen und die Besetzung von schwarzen Stadtvierteln. Sie verbergen Schichten historischer und anhaltender Diskriminierung, die die Input-Daten und Design-Annahmen automatisierter Entscheidungssysteme prägen, unter einer täuschend einfachen Bewertung." Dieser „rassistische Minimalismus" führe dazu, dass Diskriminierung zunehmend unentdeckt bleibe, dabei aber nicht weniger tödlich sei. Auch Kate Crawford vom AI Now Institute an der New York University warnt davor, dass Software durch den Bezug auf historische Daten einen „Teufelskreis" fortsetze, „indem die Polizei ihre Präsenz an den Orten erhöht, an denen sie bereits tätig ist oder überproportional patrouilliert". In diesen Gebieten fänden dann immer mehr Verhaftungen statt.

„Operation LASER" wurde mittlerweile gestoppt. In einem Memo kündigte der Polizeichef Michel Moore bereits an, zukünftig auf „Precision Policing" umzuschwenken – ein älteres, relativ schwammiges Konzept, das einerseits wie Predictive Policing den Fokus auf die kleine Gruppe von Schwerkriminellen legt, andererseits auf die Zusammenarbeit mit der „Community" setzt (Peteranderl, Die Verbrecherjagd der Zukunft ist schon gescheitert, www.spiegel.de, 22.12.2019).

USA

Mit Bluetooth gegen Unterrichtsschwänzer

Die University of Missouri (MU) verwendet eine Kombination aus versteckter Trackingtechnik und einer speziellen App, um zu überprüfen, ob Studierende ihrer Anwesenheitspflicht nachkommen. Laut Angaben der Sportabteilung der Hochschule wird das System dort seit 2016 eingesetzt – für Erstsemester ebenso wie für solche Studierende, die akademische Probleme haben. Im Rahmen eines Testprogramms soll gemäß Presseberichten das Verfahren nun auf alle „Erstis" ausgedehnt werden. Es werde ihnen mitgeteilt, dass die Überwachung ihrer Anwesenheit erfolgt, so Mitarbeiter der Hochschule. Einen „Opt-out" werde es jedoch nicht geben. Man wolle die alten Anwesenheitslisten komplett durch App und Tracking ersetzen. Allerdings dementierte die MU mittlerweile: Die Teilnahme an dem Piloten sei „optional". Man decke nur „weniger als zwei Prozent" aller Studenten an der University of Missouri ab.

Technisch umgesetzt wird die Studierendenerfassung mit einer App namens „Spotter". Diese stammt selbst von einem ehemaligen Basketballtrainer der Universität. Sie kombiniert Nahbereichssensoren im Smartphone mit dem auf dem Campus installierten WLAN-Netzwerk, hieß es. Verwendet werden dabei sogenannte Beacons, kleine Sender- und Empfangsanlagen, die in jedem Raum vorhanden sind. Umgehen lässt sich das Verfahren, indem man beispielsweise seinen Bluetooth-Empfang abdreht. Doch dann erinnert die App den Nutzer daran, dies doch bitte zu unterlassen (Schwan, Tracking-App: Mit Bluetooth gegen Schwänzer, www.heise.de 30.03.2020, Kurzlink: https://heise.de/-4666310).

USA

Inhaltskontrollen bei Apples iCloud

Mindestens seit Herbst 2019 überprüft Apple iCloud offenbar auf illegale Inhalte. Aus einem Durchsuchungsbeschluss geht hervor, dass E-Mails mit Anhängen, die gemäß dem Apple-System als bekanntes Material mit Fotos oder Videos, die Kindesmissbrauch zeigen, identifiziert werden, automatisch blockiert werden. Der Konzern setze dafür auf Hashes und einen automatisierten Abgleich mit entsprechenden Datenbanken. Ähnlich sollen auch andere IT-Konzerne vorgehen.

Ein Mitarbeiter von Apple sichtet gemäß dem Beschluss markierte E-Mails anschließend und meldet den Fall bei Verdacht auf Kinderpornographie direkt an die zuständigen US-Behörden. Übermittelt werden demnach auch Name, Adresse und Telefonnummer des verdächtigten iCloud-Nutzers. Eine Person hatte 8 E-Mails stets an den gleichen Empfänger verschickt, „die wir abgefangen haben", wird der Apple-Mitarbeiter aus den Unterlagen zitiert. Der Absender habe die Bilder wohl an sich selbst geschickt und den Vorgang mehrfach wiederholt, weil diese nicht angekommen sind, oder er sei vom Empfänger darauf hingewiesen worden. Strafverfolger haben den Unterlagen zufolge im nächsten Schritt E-Mails, Textnachrichten und alle weiteren iCloud-Dateien des Nutzers von Apple angefordert – und im Gegenzug Anfang Februar eine Datei von dem Konzern erhalten, deren Inhalt nicht im Detail aufgeführt wurde.

Anfang Januar 2020 bestätigte Apple erstmals öffentlich, dass „bestimmte Techniken" im Kampf gegen Kindesmissbrauch eingesetzt werden. Man nutze „elektronische Signaturen um vermeintlichen Kindesmissbrauch aufzuspüren". Weitere Details wurden nicht genannt. Auf eine „Vorabprüfung und das Scannen hochgeladener Inhalte auf potenziell illegale Inhalte" weist Apple seit Herbst 2019 in der Datenschutzrichtlinie hin. Auf welche weiteren „illegalen Inhalte" das System dabei achtet, ist unklar. Offen bleibt auch, ob Apple einen Weg gefunden hat, Material zu prüfen, das über den Ende-zu-Ende-verschlüsselten Messaging-Dienst iMessage ausgetauscht wird.

US-Behörden haben ihr Vorgehen gegen Verschlüsselung jüngst wieder verstärkt – besonders mit dem Verweis auf Kindesmissbrauch. US-Justizminister William Barr forderte Facebook im Herbst 2019 dazu auf, Strafverfolgern Inhaltszugriffe zu ermöglichen; nur so könne man Kinder schützen. Das Netzwerk hatte zuvor in Aussicht gestellt, auch Facebook Messenger durch Ende-zu-Ende-Verschlüsselung abzusichern. Barr kritisierte Anfang Januar 2020 Apple scharf, weil der Konzern nicht bei der Entsperrung eines verschlüsselten iPhones helfen wolle; Apple wies die Vorwürfe zurück (Becker, Apple-Mitarbeiter prüfen E-Mails bei Verdacht auf Kindesmissbrauch, www.heise.de 13.02.2020, Kurzlink: https://heise.de/-4660126)

Australien

Mobilgeräte-Detektor-Einsatz bei Kfz-Nutzung

Im australischen Bundesstaat New South Wales sind Ende 2019 Überwachungskameras regulär in Betrieb genommen worden, die nicht nur erfassen, ob Kfz-Nutzende zu schnell fahren, sondern auch erkennen, ob sie sich am Steuer korrekt verhalten. Gemäß der zuständigen Behörde (Transport for NSW) handelt es sich um die weltweit ersten Handy-Erkennungskameras, die Tag und Nacht bei allen Wetterbedingungen arbeiten, um festzustellen, ob ein Fahrer ein Mobiltelefon bedient. Gemäß dem zuständigen Polizeichef ist das „ein System, um die Kultur zu verändern".

Das System verfüge über eine Reihe Kameras und einen Infrarotblitz, um bei allen Verkehrs- und Wetterbedingungen klare Bilder von vorbeifahrenden Fahrzeugen aufzunehmen. Möglich sein sollen fest installierte und mobile Kontrollen, die alle auf der gleichen Technologie basieren. Die Aufnahmen der Überwachungskameras werden mit sog. künstlicher Intelligenz ausgewertet. Sobald die Algorithmen eine wahrscheinlich illegale Nutzung von Mobilgeräten erkennen, werden die Bilder durch Menschen überprüft.

Die Autofahrer-Überwachung hat sich angeblich in einem Pilotprojekt von Januar bis Juni 2019 bewährt. Dabei wurden gemäß Behördenangaben über 100.000 Fahrerinnen und Fahrer erwischt, die im Auto ein Mobiltelefon illegal verwendeten. Wie bei anderen Programmen für Verkehrsüberwachungskameras gäbe es „strenge Kontrollen, um sicherzustellen, dass die vom System erfassten Bilder sicher gespeichert und verwaltet werden". Die australischen Behörden setzen stark auf digitale Mustererkennung. So wurde Oktober 2019 bekannt, dass das australische Innenministerium an einem Gesichtserkennungsdienst zur Altersverifikation arbeitet, der von Porno- und Glücksspiel-Webseiten eingesetzt werden soll. Damit würde das bereits bestehende staatliche Gesichtserkennungssystem für die Privatwirtschaft geöffnet.

Es wurde angekündigt, dass in den ersten drei Monaten des Einsatzes der Mobilnutzungserkennung fehlbare Fahrerinnen und Fahrer nur eine Verwarnung erhalten sollen. Danach müsse die vom Gesetzgeber vorgesehene Geldstrafe von umgerechnet rund 210 € bezahlt werden. In einer Schulzone würden ca. 280 € fällig. Zudem gibt es Strafpunkte, die ab einer bestimmten Anzahl zum Ausweisentzug führen. Sprachanrufe während der Fahrt sind nur mit einer Freisprecheinrichtung erlaubt. Alle anderen Tätigkeiten, wie etwa Videoanrufe, die Nutzung von Social Media oder das Fotografieren, sind während der Fahrt verboten. Verkehrsminister Andrew Constance erklärte: „Wer denkt, weiterhin die eigene Sicherheit, die von Mitfahrern und der Gesellschaft ohne Folgen gefährden zu können, den erwartet eine böse Überraschung." Bisher seien bis Dezember 2019 329 Menschen auf den Straßen von New South Wales gestorben, verglichen mit 354 Menschen im gesamten vorangegangenen Jahr, so die offizielle Statistik (Handysündern geht es an den Kragen: Diese Kamera erkennt, wenn du am Steuer telefonierst, www.watson.ch 02.12.19).

Technik-Nachrichten

Verizon geht mit datenschutzfreundlicher Suchmaschine auf den Markt

Verizon Media startet mit OneSearch eine neue Suchmaschine, die den Fokus auf den Datenschutz legt. OneSearch soll so gut wie nichts über die Nutzenden speichern. Im automatisch voreingestellten Advanced Privacy Mode löscht sie nach einer Stunde sogar den verschlüsselten Link zu den Suchergebnissen. Dahinter steckt das Unternehmen Verizon Media, Basis ist Bing, die Suchmaschine von Microsoft.

Alle Anfragen werden verschlüsselt. Die Suchmaschine speichert keine Verläufe, IP-Adressen und Standorte. So ist es nicht möglich, Nutzerprofile zu erstellen. Die Ergebnisse werden daher auch nicht an den Nutzer angepasst, wie es z.B. bei Google der Fall ist. Es gibt kein Cookie-Tracking oder Retargeting. Da keine Daten gespeichert werden, können sie auch nicht an Werbetreibende weitergeleitet oder verkauft werden. Die Werbeanzeigen sind nicht personalisiert, sondern sind auf

Grundlage der aktuellen Suchanfrage kontextbasiert.

Bisher ist OneSearch als Desktop- und Mobile-Web-Variante für Nordamerika optimiert, sie lässt sich aber auch in Europa testen. Neben der Auswahl zwischen Textquellen, Bildern und Videos, kann man eine Art Kinder-Sicherheit einstellen: „kein Filter", „keine expliziten Bilder" und „keine Erwachsenenbilder". Die Suchmaschine soll sich künftig auch von anderen Unternehmen in die eigenen Produkte integrieren lassen. Ein Start-Termin für andere Regionen ist noch nicht bekannt. iOS- und Android-Versionen sollen in Kürze erscheinen.

Hauptkonkurrenz für OneSearch ist in Nordamerika DuckDuckGo, das ähnlich auf den Datenschutz fokussiert, keine Informationen weitergibt und Tracker blockiert. In Europa ist Startpage als datenschutzfreundliche Alternative zu GoogleSearch oder Bing verbreitet. Ab März 2020 steht DuckDuckGo beim Einrichten eines Android-Geräts als Standard-Suchmaschine zur Auswahl. Google durfte nach einem EU-Urteil nicht weiter nur die hauseigene Suchmaschine anbieten. Zum Mutterkonzern Verizon gehören auch Yahoo und AOL. Die New Yorker betreiben die beiden Unterseekabel Ulysses 1 und 2. Zu den Enthüllungen Edward Snowdens gehörte auch, dass Verizon der NSA Verbindungsdaten zugänglich machte. Dafür bekam das Unternehmen dicke Zahlungen. Auch der Deutsche Bundestag nutzte Verizon als Provider, beendete aber 2014 die Zusammenarbeit kurz nach Bekanntwerden der NSA-Kooperation (Weiß, Fokus auf Datenschutz: Verizon Media startet Suchmaschine OneSearch, www.heise.de 27.01.2020; Kurzlink: https://heise.de/-4646378).

Samsung-Smartphones telefonieren eigenständig nach China

Die auch auf neuen Samsung-Smartphones vorinstallierte App Device Care schickt Daten zu einem chinesischen Sicherheitsunternehmen. Die Software dient Wartungszwecken. Sicherheitsforscher haben entdeckt, dass die App Kontakt mit einem chinesischen Server aufnimmt und Daten übermittelt, ohne dass die Nutzenden dem explizit zustimmen müssen. Was das chinesische Unternehmen mit den Daten macht, ist nicht bekannt.

Die vorinstallierte App Device Care kann von einem normalen Nutzer auch nicht deinstalliert werden. Die Daten landen beim Unternehmen Qihoo360. Was für Daten an diese chinesische Firma gehen, ist nicht bekannt. Dieses fragwürdige Verhalten hatte ein Reddit-Nutzer entdeckt, während er die Kommunikation seines Smartphones Galaxy S10+ mit dem Netzwerkscanner Wirescan untersuchte.

Samsung teilte mit, dass die App lediglich den Typ des Smartphones, dessen Speicherkapazität und die Android-Version verrät, es sich dabei also um keine personenbezogenen Daten handele. Sie überwache den Speicher der Samsung-Geräte und erkenne sogenannte Junk-Dateien, die nur Platz verbrauchen, aber nicht mehr benötigt würden. Qihoo360 stellt eine Datenbank mit solchen Dateien zur Verfügung, die die App nutzt. Qihoo360 hat keinen guten Ruf. Das Unternehmen fiel in der Vergangenheit mehrmals in Sicherheitskreisen negativ auf. So verkauft das Unternehmen eine Anti-Virus-Software, die Anwendungen der Konkurrenz als Viren markiert und diese entfernt. Außerdem hat das Unternehmen eine Browserleiste im Programm, die Werbung einblendet und fälschlicherweise vor einem Virus warnt und die Installation der eigenen Anti-Virus-Lösung anbietet (Gundlach, Datenschutz: Samsung-App schickt Daten ungefragt nach China, www.maclife.de 10.01.2020).

Gesundheitscheck mit der intelligenten Toilette

Forschende von der US-Universität Stanford haben eine smarte Toilette entwickelt, die Kot und Urin medizinisch analysieren und die jeweiligen Benutzer biometrisch identifizieren können soll. Sie haben dafür eine normale Toilette vernetzt und mit allerhand Analysetechnik ausgestattet: Kameras, Druck- und Bewegungssensoren. So sollen sich Erkrankungen wie Prostata-Krebs oder Nierenprobleme schneller diagnostizieren lassen. Die Toilette erfasst beim Erledigen der Geschäfte die sogenannte Urodynamik, was unter anderem Durchflussrate und Druck des Urinstahls beinhaltet, ebenso wie die Konsistenz des Stuhls. Zudem kommen Teststreifen zum Einsatz, die molekulare Eigenschaften des Urins ermitteln. Gemäß Studienleiter Sanjiv Gambhir kann die Toilette zehn verschiedene Biomarker messen. Getestet wurde das Experimentalklo in einer Studie mit 21 Personen.

Die ermittelten Daten sollen automatisiert in einem sicheren Cloudsystem abgelegt werden können, damit sie für Ärzte und Gesundheitseinrichtungen bereitstehen. Die Toilettensysteme sollen autonom funktionieren und auch von mehreren Personen benutzt werden. Daher sehen die Forscher auch die Notwendigkeit einer Identifikation der Nutzer, damit Daten richtig zugeordnet werden. Hierfür wurde in der Spültaste ein Fingerabdruckleser integriert. Für den Fall, dass jemand anders die Spülung drückt, haben die Forschenden ein Kamerasystem für die Anus-Erkennung eingebaut, damit Nutzer anhand von Aufnahmen ihrer Analregion identifiziert werden können. Gambhir: „Es zeigte sich, dass es auch einen einzigartigen Anus-Abdruck gibt." Entsprechende Aufnahmen dienten aber nur der Erkennung und seien nicht für die Speicherung und Weiterleitung an die Ärzte vorgesehen, so die Pressemitteilung.

Unklar ist, ob diese Technik Serienreife erreicht und den Weg in private Badezimmer findet. Eine Umfrage unter 300 Personen habe laut den Forschern ergeben, dass sich rund 37% der Befragten halbwegs vorstellen könnten, eine solche Toilette zu benutzen (Kannenberg, Smarte Toilette mit Anus-Erkennung und Fäkalienanalyse, www.heise.de 08.04.2020, Kurzlink: https://heise.de/-4699245).

Rechtsprechung

KG Berlin

Facebook verstößt gegen Datenschutzrecht

Das Kammergericht Berlin (Oberlandesgericht) hat mit Urteil vom 20.12.2019 in einem Verfahren gegen Facebook das Urteil des Landgerichts Berlin vom 16.01.2018 (DANA 1/2018, 760 f.) bestätigt (Az. 5 U 9/18) und stärkt damit die Position des Verbraucherzentrale Bundesverbands (vzbv). Auf die Berufung hin bestätigte das Gericht, dass Facebook mit seinen Voreinstellungen zur Privatsphäre und einem Teil seiner Geschäftsbedingungen gegen Verbraucher- und Datenschutzrecht verstößt. Das soziale Netzwerk muss dies unterlassen.

Der vzbv hatte 2015 insgesamt 26 Einzelverstöße beanstandet. Die Verbraucherschützer monierten unter anderem den im Smartphone standardmäßig aktivierten Ortungsdienst von Facebook, der auch Chat-Partnern den Aufenthaltsort verriet, sowie den erlaubten Zugriff von Suchmaschinen auf die Nutzerfeeds. Für beides hätte laut Gericht eine Einwilligung, also ein Opt-in, erfordern müssen.

Die Klauseln, dass Facebook sich die Nutzung des Namens und Profilbilds von Mitgliedern für „kommerzielle, gesponserte und verwandte Inhalte" vorbehält und Nutzer sich vorab mit allen Änderungen der Datenrichtlinien einverstanden erklären hätten müssen, hielten die Richter für nicht haltbar. Auch die Klarnamenpflicht hat in den Augen des Gerichts keinen Bestand. Der vzbv erläutert: „Eine Klausel, die Nutzer unter anderem zur Angabe ihres richtigen Namens verpflichtete, ist dem Unternehmen nach teilweiser Berufungsrücknahme im Dezember 2019 bereits jetzt rechtskräftig untersagt."

Facebook hatte sich auch dagegen gewehrt, dass der Verband überhaupt klagen darf. Mit Inkrafttreten der DSGVO brauche es dafür den Auftrag eines betroffenen Verbrauchers. Auch dies sah das Gericht anders: Es ist „Verbänden zur Wahrung von Verbraucherinteressen ausdrücklich gestattet, gegen den mutmaßlichen Verletzer von Vorschriften zum Schutz personenbezogener Daten vorzugehen." Beanstandet wird vom Gericht auch das versteckte Impressum.

vzbv-Rechtsreferent Heiko Dünkel begrüßte das Urteil: „Nicht zum ersten Mal wird Facebook wegen des sorglosen Umgangs mit den Daten seiner Nutzerinnen und Nutzer verurteilt." Das Kammergericht habe dabei klargestellt, dass Verbraucherzentralen dagegen vorgehen könnten.

Nicht beanstandet hat das Gericht den damaligen Werbeslogan „Facebook ist und bleibt kostenlos". Der vzbv hatte ihn als irreführend kritisiert, da Verbraucher zwar kein Geld für den Dienst zahlen müssen, wohl aber mit ihren Daten bezahlen, die Facebook Gewinn einbringen. Nach Auffassung des Kammergerichts bezieht sich die Werbung jedoch nur darauf, dass die Dienste ohne Geldzahlungen oder andere Vermögenseinbußen genutzt werden können. Der Senat wies außerdem die Klage gegen einzelne Klauseln aus der Datenrichtlinie des Unternehmens ab. Bei diesen handele es sich nicht um Allgemeine Geschäftsbedingungen.

Eine Revision hat das Gericht nicht zugelassen. Allerdings können beide Parteien eine Nichtzulassungsbeschwerde beim Bundesgerichtshof einreichen. Eine Facebook-Sprecherin kommentierte das Urteil: „Unabhängig von diesem Verfahren haben wir unsere Geschäftsbedingungen und Datenrichtlinie im Frühjahr 2018 umfassend überarbeitet. In seiner Pressemitteilung verweist der VZBV auf mehrere Klauseln und Einstellungen, die in dieser Form schon längst nicht mehr existieren, aber in einem seit 2015 anhängigen Verfahren formal nach wie vor zur Entscheidung standen." (Weiß, Urteil: Facebook verstößt gegen Daten- und Verbraucherschutz, www.heise.de 24./27.01.2020, Kurzlink: https://www.heise.de/-4645477; Facebook verstößt gegen Datenschutzrecht, www.vzbv.de 24.01.2020).

LG Heidelberg

Kein Auskunftsanspruch bei zu hohem Aufwand

Gemäß einem Urteil des Landgerichts (LG) Heidelberg vom 21.02.2020 besteht das Auskunftsrecht nach Art. 15 Datenschutz-Grundverordnung (DSGVO) nicht, wenn eine Auskunft vom Verantwortlichen nur mit unangemessenem Aufwand erteilt werden kann (Az. 4 O 6/19). Im konkreten Fall wäre eine Sichtung und Schwärzung von ca. 10.000 E-Mails nötig gewesen. Der Kläger war ehemaliges Vorstandsmitglied einer Aktiengesellschaft. Diese meldete Insolvenz an und der Beklagte wurde zum Insolvenzverwalter bestellt. Der Kläger berief sich nun auf Art. 15 DSGVO und verlangte einen umfassenden Auskunftsanspruch. Hilfsweise verlangte er Auskunft über die E-Mail-Korrespondenz innerhalb eines bestimmten Zeitraums.

Das LG Heidelberg wies beide geltend gemachten Ansprüche als unbegründet ab.

Der umfassende Auskunftsanspruch sei viel zu weitreichend und zu unbestimmt, so das Gericht:

„Art. 15 DSGVO gewährt einen Anspruch auf Auskunftserteilung der personenbezogenen Leistungs- und Verhaltensdaten. Bei personenbezogenen Leistungs- und Verhaltensdaten handelt es sich um eine bestimmte Kategorie von personenbezogenen Daten i.S.v. Art. 15 Abs. 1 Hs. 2 b) DSGVO i.V.m. Art. 4 Nr. 1 DSGVO (...).

Vorliegend beschreibt der Kläger jedoch nicht einmal, auf welche Bereiche bzw. Kategorien er seine Auskunft erstrecken lassen will. Für Verantwortliche, die eine große Menge von Informationen über die betroffene Person verarbeiten, sieht Erwägungsgrund 63 a.E. zunächst eine Erleichterung bei einem (pauschalen) Auskunftsersuchen vor. So darf der Verantwortliche vor Auskunftserteilung von der betroffenen Person eine Präzisierung des Auskunftsbegehrens verlangen (s. auch Bäcker in

Kühling/Buchner DSGVO Art. 15 Rn. 30; Schantz in Schantz/Wolff DatenschutzR Rn. 1193; bzgl. der Herausforderungen iRv Big Data Anwendungen s. Werkmeister/Brandt CR 2016, 233 (236 f.)).

Die betroffene Person hat klarzustellen, an welchen Informationen bzw. welchen Verarbeitungsvorgängen sie interessiert ist (Paal/Pauly/Paal, 2. Aufl. 2018, DSGVO Art. 15 Rn. 8)."

Der Hilfsanspruch hinsichtlich der Herausgabe der E-Mails sei zwar ausreichend bestimmt, scheitere aber daran, dass dieser unverhältnismäßig sei. Denn für die Sichtung und Schwärzung der E-Mails würden Kosten iHv. mehr als 4.000 EUR entstehen. Darüber hinaus würde die Durchführung der Auskunft die Ressourcen des Beklagten über Wochen binden. Das Informationsbegehren des Klägers sei im vorliegenden Fall deutlich geringer einzustufen als die berechtigten Interessen des Unternehmens. Darüber hinaus handle es sich um elektronische Nachrichten, die zwischen 9-10 Jahre zurückliegen würden. Auch der Kläger selbst sei seit 9 Jahren nicht mehr bei der insolventen Firma beschäftigt.

Das LG Heidelberg wertete es insbesondere nachteilig für den Kläger, dass er seinen Auskunftsanspruch erst Jahre später im Rahmen eines zivilrechtlichen Verfahrens geltend machte. Ebenso zog das Gericht nachteilige Schlüsse aus dem Umstand, dass der Kläger, obgleich persönlich geladen, nicht selbst erschien, sondern unentschuldigt fernblieb.

Das Urteil steht in einem gewissen Spannungsverhältnis zu einem Urteil des Landesarbeitsgerichts Stuttgart vom 20.12.2018, wo ein ehemaliger Mitarbeiter der Rechtsabteilung den Daimler-Konzern auf umfassende DSGVO-Auskunft verklagte und Recht bekam (Az. 17 Sa 11/18) (Zöll/Kielkowski, Zuviel Aufwand? Kein Auskunftsanspruch nach DSGVO!, blog.handelsblatt.com 09.03.2020; Bahr, Kein DSGVO-Auskunftsanspruch, wenn Aufwand zu-hoch (hier Sichtung von ca. 10.000 E-Mails), www.dr-bahr.com 09.03.2020).

Buchbesprechungen



Krahmer, Utz (Hrsg.)
Sozialdatenschutzrecht
Persönlichkeitsschutz nach SGB I, SGB X, DSGVO
4. Aufl. Nomos Baden-Baden, 2020,
ISBN 978-3-8487-3056-8, 488 S., 78 €

(tw) So üppig die Literatur zur allgemeinen Umsetzung der europäischen Datenschutz-Grundverordnung (DSGVO) ist, so dürftig war sie in Bezug auf die spezifische Umsetzung im Sozialrecht. Abgesehen von einer Artikelserie von Bieresborn in der Neuen Zeitschrift für Sozialrecht zum Jahreswechsel 2017/2018 gab es lange überhaupt nichts. Inzwischen erscheinen die ersten Neuauflagen der Kommentierungen zu einzelnen Sozialgesetzbüchern (SGB). Es ist nun das Verdienst des Nomos-Verlags, die Lücke zu schließen und eine umfassende Kommentierung der Datenschutzregelungen im SGB I und SGB X vorzulegen. Eine weitere, eher auf die Praxis ausgerichtete Veröffentlichung, herausgegeben von Kipker/Voskamp, ist angekündigt.

Wie wichtig eine qualifizierte Kommentierung der nach der DSGVO überarbeiteten Regelungen ist, ist für diejenigen, die mit der Thematik zu tun haben, offensichtlich: War das Ineinandergreifen von allgemeinem Datenschutzrecht und SGB schon kompliziert genug, so kommt nun mit der DSGVO eine weitere Ebene hinzu. Zwar können, dank der Öffnungsklauseln in der DSGVO, sowohl Struktur und Inhalte der SGB-Regelungen beibehalten werden – und an dieser Vorgabe hat sich der Bundesgesetzgeber in teilweise erschreckender Weise orientiert – doch wird das Wechselspiel zwischen SGB I und X, den speziellen SGB-Regelungen und dem allgemeinen Datenschutzrecht, das im BDSG und vorrangig nun in der DSGVO zu finden ist, noch anspruchsvoller. Dazu beigetragen hat, dass die DSGVO hier nicht beim gängigen Namen benannt wird, sondern juristisch als „Verordnung (EU) 2016/679" geführt wird, was fast so giftig klingt wie „E 605".

Dem Kommentar gelingt dann aber in einer zumindest für Juristen nachvollziehbaren Weise die Darstellung dieses Wechselspiels, indem der das Sozialgeheimnis regelnde § 35 SGB I und die §§ 67 bis 85a SGB X ausführlich kommentiert werden. Dabei gehen die Kommentierungen nach einem bewährten Muster vor: Gegenstand und Aufbau der Norm (Rn. 1), europarechtlicher Kontext (Rn. 2), Entstehungsgeschichte (Rn. 3), Gesetzesmaterialien (Rn. 4) und dem folgend die Erläuterung des Normwortlautes. Besonders wertvoll ist der Abdruck der Gesetzesmaterialien, was dem Rechtsanwender oft klarmacht, welche und wie wenig Gedanken sich der Gesetzgeber gemacht hat, als er die Paragrafenungetüme schuf. Auch die Wechselbezüge zum spezifischen Sozialrecht, etwa dem SGB VIII zur Kinder- und Jugendhilfe, werden exemplarisch dargestellt. Da die vorliegende Kommentierung auf Vorauflagen (in anderen Verlagen) zurückgreift, wird ausführlich auch die ältere Literatur dargestellt, was für das aktuelle Verständnis der Regelungen oft hilfreich ist.

Äußerst erfreulich ist das recht vollständige Literaturverzeichnis. Die Struktur des SGB X in den §§ 67 ff. folgt zwar der bisherigen gesetzlichen Logik, doch fällt es dann doch schwer, angesichts der oft verschwurbelten Gesetzesformulierungen den konkret anwendbaren Text und die dazu gehörende Kommentierung zu finden, so dass dann das Stichwortverzeichnis und die gute Gliederung hilfreich sind.

Also: Ein rund herum gelungenes Werk. Es ist das Ergebnis der akribischen Arbeit der wenigen ausgewiesenen Expertinnen und Experten, von denen hier viele zu Wort kommen: Ahrend, Dix, Hoffmann, Hoidn, Kipker, Krahmer, Kreße, Meißner, Raum, Sommer und Strothmann. Dennoch ist etwas Kritik erlaubt: Zum einen wäre es schon zu wünschen gewesen, dass die für den Rechtsanwender oft unzumutbaren Regelungen, was zu Vollzugsdefiziten führt, als solche benannt worden wären. Auch rechtspolitische Kritik wäre angebracht und hätte der dogmatischen Darstellung nicht geschadet. Schließlich gibt es kleine dogmatische Unzulänglichkeiten, etwa wenn die jüngste Änderung zur beruflichen Schweigepflicht in § 203 StGB zu kurz kommt. Für Juristinnen und Juristen, die mit Sozialdatenschutz zu tun haben, wird das Buch vorläufig wohl das Standardwerk sein, auf das man vertrauensvoll zurückgreifen kann.



Huber, Christian/Kornes, Roland/
Mathis, Melanie/Thoenneßen, Axel
(Hrsg.)
Tagungsband „Fachtagung Personenschaden 2019“
Baden-Baden 2019, Nomos Verlag,
ISBN 978-3-8487-6312-2

(me) Unter der Ägide des Instituts für faire Schadensregulierung GmbH fand am 7. und 8. November 2019 die „Fachtagung Personenschaden 2019“ statt.

Zweck und Ziel von Tagung und dazugehörendem Tagungsband soll es sein, über die aktuelle Rechtsprechung des Verkehrsunfallrechts, Arzthaftungsrechts und Sozialversicherungsrechts zu informieren und darüber hinaus ein größeres Thema in den Mittelpunkt zu stellen. Bei diesem größeren Thema handelt es sich aus Sicht des datenschutzrechtlich Interessierten um einen besonderen Leckerbissen:

Großflächige Belegforderungen und Datenerhebungen der Assekuranzunternehmen durch ihren Dienstleister (Actineo) im Zuge der Geltendmachung von Regressforderungen der Sozialversicherungsträger.

Zu diesem Thema gab es drei größere Vorträge, von denen zwei in den Tagungsband aufgenommen wurden. Im ersten führt Roland Kornes sehr ausführlich und lehrreich in das Thema ein. Sein Referat hat den Titel „Belegforderungswelle und massive Datenerhebungen bei Regress-Forderungen“. Der Referent schildert das von ihm so genannte „Regulierungs-Klima“ aus Sicht der Sozialversicherungsträger. Es geht um den Interessenausgleich zwischen Geschädigtem und seinem Sozialversicherungsträger auf der einen und dem Schädiger und seiner Haftpflichtversicherung auf der anderen Seite. Problematisch wird dieser Vorgang, weil der Haftpflichtversicherer einen externen Dienstleister einschaltet. Dies ist wohl vorwiegend die Firma Actineo GmbH, die sich selbst als „deutschen Marktführer für die Digitalisierung und medizinische Einschätzung von Personenschäden“ bezeichnet. Actineo fordert im Regulierungsfall die „umfassende Belegung sämtlicher Forderungen und Rechnungspositionen“, was nicht nur aus datenschutzrechtlicher Sicht problematisch erscheint. Dadurch kommt es für die Sozialversicherung zu erhöhten Kosten und für den Geschädigten zu einer nicht unerheblichen Verzögerung bei der Schadensregulierung. Kornes legt dar, welche Belegpflichten für die Sozialversicherung rechtlich vorgesehen sind und inwieweit das Vorgehen der Firm Actineo problematisch, ja rechtlich anzuzweifeln ist, was z.T. datenschutzrechtlich begründet sein kann. Sehr schön ist in diesem Zusammenhang die Darlegung einschlägiger Gerichtsurteile. Kornes überzeugt durch die Verwendung von Beispielen, die auch dem des Regressrechts Unkundigen einen guten Zugang zur Materie verschaffen. Außerdem lässt die nicht humorlose Auswahl der Überschriften die Empörung des Fachmannes deutlich werden: Da wird vom „Regulierungs-Ozean“ und „Belegforderungs-Tsunami“ gesprochen und dies anschaulich belegt. Beachtenswert sind die Ausführungen zu den Datenschutzbedenken des Referenten, der auf „datengetriebene Verhaltenstarife in der Versicherungswirtschaft“ und auf die Gefahr der Verknüpfung mit anderen Risikobereichen hinweist. In völliger Intransparenz für den Kunden werden Daten aufgezeichnet und von einem Dienstleister 5 Jahre, von der Versicherung 10 Jahre gespeichert (und wohl auch verwendet), was mehr als bedenklich ist.

Der zweite Vortrag von Hülsmann schließt sich thematisch an die Ausführungen des ersten Referenten an und ist für am Datenschutz Interessierte sehr lesenswert! Der Referent entwirft eine inhaltlich und stilistisch überzeugende Betrachtung zur Sammlung und Verarbeitung von Gesundheitsdaten durch Haftpflichtversicherungen und ihre Dienstleister am Beispiel der Firma Actineo GmbH. Besonders lohnend ist dieser Beitrag, weil er zunächst die Voraussetzungen einer rechtmäßigen Datenverarbeitung darlegt, die besondere Stellung der Gesundheitsdaten beleuchtet und die von der Rechtsordnung vorgesehenen Möglichkeiten einer Weitergabe personenbezogener Daten an Dritte beschreibt. Damit sind die Grundlagen der Verarbeitung personenbezogener Daten auf eine Art und Weise erläutert, dass selbst der nicht täglich mit datenschutzrechtlichen Fragen befasste Jurist und Informatiker verstehen kann, wie problematisch die Vorgehensweise des Auftragsverarbeiters Actineo ist. Hülsmann zeigt auf, dass die von Actineo angebotene „Auftragsverarbeitung“ den rechtlichen Rahmen des Art. 28 DSGVO sprengt und einen

Großteil der Daten wohl eher für eigene Zwecke ge- bzw. missbraucht. Vielen Lesern dürfte Hülsmann aus der Seele sprechen, wenn er den Irrweg des deutschen Gesundheitswesens beschreibt, das zu einer „renditeorientieren Gesundheitswirtschaft" mutiert ist. Dazu passt die fragwürdige Einbindung einer „Auftragsverarbeitung" bei der Schadensregulierung durch Dienstleister, die dabei Eigennütziges und möglicherweise Rechtswidriges im Schilde führen, um „Deutschlands größte unabhängige Datenbank medizinisch codierter Personenschäden" zu schaffen. Sehr schön ist der Verweis auf das Volkszählungsurteil des Bundesverfassungsgerichts, wonach die betroffene Person eben nicht zum bloßen Objekt reduziert werden darf, das keine Befugnis mehr hat, selbst über Preisgabe und Verwendung seiner Daten zu bestimmen. So wird die abschließend von Hülsmann gestellte Frage nach der Legalität und Legitimität der Datenverarbeitung durch den genannten Dienstleister zu Recht erhoben. Eine Befassung der Angelegenheit durch die Datenschutzaufsichtsbehörde wäre zu wünschen! (der Vortrag findet sich auch in DANA 1/2020, 13-19).

In einem dritten kleineren Beitrag bewertet Thoenneßen die „Belegforderung durch die Actineo GmbH aus zivilprozessualer Sicht". Empathisch vergleicht der Referent die Vorgehensweise der Haftpflichtversicherer gegenüber den Sozialversicherungsträgern mit der Vorgehensweise bei Kfz-Blechschäden, bei der ebenfalls „Prüf-Organisationen" zum Angriff gegen die Berechnungen des Geschädigten eingesetzt werden. Unter Heranziehung einschlägiger Gerichtsurteile empfiehlt Thoenneßen eine Vorgehensweise, die mit verzugsbedingter Fristsetzung und baldiger Klageerhebung ökonomischer ist als langwierige vorgerichtliche Auseinandersetzungen mit den Haftpflichtversicherern.

Nicht unerwähnt bleiben sollen der zweite und dritte Themenkomplex: Dabei geht es um eine der wesentlichsten Fragen des Zivilprozesses, nämlich die Beweislast, die vom Referenten Scholten als „Zünglein an der Waage" bezeichnet wird und überaus entscheidungserheblich ist. Verdienstvoll ist die Erläuterung von primärer und sekundärer Darlegungslast sowie der Fragen, die im Schadensersatzprozess regelmäßig abzuarbeiten sind, wie beispielsweise Schmerzensgeld, Heilbehandlungskosten, Verdienstausfall, um nur einige zu nennen. Während Scholten aus Sicht des Richters vorträgt, führt die nachfolgende Referentin Mathis die Problematik aus Sicht der Anwältin aus. Beides ist für den Praktiker überaus nützlich und lesenswert.

Im dritten und letzten Teil geht es darum, aktuelle Rechtsprechungsbeispiele zu den Themata „Personenschaden", „Haftungsprivilegierung beim Arbeitsunfall" und „Arzthaftpflicht" zu erläutern. Die Übersicht muss als gelungen bezeichnet werden. Sie ist gut geschrieben und erfüllt den im Geleitwort des Tagungsbandes beschriebenen Zweck: nämlich im halbjährlichen Abstand die bedeutendsten Entscheidungen des letzten Halbjahres darzustellen und die Teilnehmer auf einen „lückenlosen Wissensstand" zu bringen.

Auf weitere Tagungen dieser Art ist der fachlich interessierte Leser gespannt.



Berger, Hannes
Öffentliche Archive und staatliches Wissen
Die Modernisierung des deutschen Archivrechts
Tectum Verlag Baden-Baden, 2019, 608 S.
ISBN 978-3-8288-4373-8, 112,00 €

(tw) Es gibt Rechtsbereiche, die von Anfang an hohe datenschutzrechtliche Relevanz hatten und weiterhin haben, ohne dass sich dies bisher in der „Literatur", also in der publizistischen und wissenschaftlichen Aufarbeitung niedergeschlagen hat. Ein solcher Bereich ist das Archivrecht, das nach der Volkszählungsentscheidung 1983 aus guten Gründen an diese neue Verfassungsrechtsprechung angepasst wurde und so eine erste Generation von Gesetzen in Bund und Ländern erhalten hat. Der gute Grund liegt darin, dass in öffentlichen Archiven die Dokumente der öffentlichen Verwaltung gelagert werden, die von „bleibendem Wert" sind; dies sind zu einem großen Teil Dokumente mit personenbezogenen Angaben. Diese Unterlagen werden zentral für die jeweilige Verwaltungsebene gespeichert und stehen grundsätzlich jedermann, also auch jeder Frau, zur Auswertung zur Verfügung.

Dass sich hieraus bisher nur wenige Datenschutzkonflikte ergeben haben, liegt daran, dass die Existenz der Archive nur wenigen Spezialisten, insbesondere Historikern, bewusst ist und dass vor ihrer Bereitstellung für die Öffentlichkeit zunächst zumeist 30 Jahre vergangen sein mussten. In unserer schnelllebigen Informationsgesellschaft interessiert diese Vergangenheit bisher nur wenige und dies äußerst selektiv. Doch wird sich die Bedeutung der Archive ändern. Zum einen werden die Sperrfristen verkürzt; teilweise dauert diese Frist oft nur noch 10 Jahre; bei Unterlagen aus dem Bereich der Informationsfreiheit sind die Sperrfristen teilweise völlig abgeschafft. Zum anderen führt die Digitalisierung der Verwaltung zu einer massiven Steigerung des Informationsanfalls, was zu völlig neuen Auswertungsmöglichkeiten und – zumindest potenziell – neuen Begehrlichkeiten führt.

Umso erstaunlicher ist, dass trotz dieses neuen Interesses seit den 80er Jahren des letzten Jahrhunderts das Archivrecht fast unverändert geblieben ist. Wohl gab es Anpassungen wegen Änderungen im Urheberrecht und im Informationsfreiheitsrecht, auch wegen neuer Möglichkeiten und Bedarfe, die sich mit der Digitalisierung ergeben. Doch sind die Umbrüche in der Politik, also bei den Gesetzgebern im Bund und in den Ländern, zumeist nur bruchstückhaft angekommen. Dies gilt selbst für den jüngsten Umbruch: die direkte Geltung der europäischen Datenschutz-Grundverordnung (DSGVO) seit Mai 2018. Die DSGVO hat wichtige Änderungen für das Archivrecht zur Folge, sie privilegiert die archivische Sekundärnutzung von personenbezoge-

nen Dokumenten und eröffnet zugleich Einschränkungsmöglichkeiten bei den Betroffenenrechten. Doch davon ließ sich die Politik nicht beeindrucken: Sie passte formal die Terminologie und einige Regeln an. Das war es dann aber auch schon. Dass dadurch offensichtlich die europäischen Rechtsvorgaben verletzt werden, scheint bisher kaum jemanden zu jucken (vgl. die Besprechung von Partsch, Bundesarchivgesetz, in DANA 4/2019, 241).

Bisher! Das muss und kann sich ändern – mit der vorliegenden Dissertation aus Erfurt. Hannes Berger liefert auf knapp 600 Seiten eine schonungslose Analyse des bestehenden Archivrechts und kommt zu dem Ergebnis, dass sich sehr viel ändern muss, wenn wir mit der Verfassungsrechtslage und der technischen Entwicklung in unserer Informationsgesellschaft Schritt halten wollen. Unaufgeregt und in einer für Nicht-Juristen verständlichen Sprache beschreibt Berger die historische Entwicklung, den aktuellen Stand und die Novellierungsnotwendigkeiten des Archivrechtes – und dies so umfassend und detailliert und zugleich so stringent, dass (fast) alle Informationsbedürfnisse befriedigt werden. So rekapituliert er die Entwicklung des deutschen Verfassungsrechts, das mit dem preußischen Arkanprinzip startete, aber dahin strebt, dem Staat ein hohes Maß an Transparenz und Informationsdienstleistung im Interesse des demokratischen Diskurses und des wissenschaftlichen Fortschritts abzuverlangen. Dabei referiert er die bisher äußerst konservativ bleibende Rechtsprechung des Bundesverfassungsgerichtes und schlägt sich auf die Seite der modernen Juristen, die in der Garantie der Informationsfreiheit eine staatliche Leistungsverpflichtung sehen. Er konstatiert aber auch, dass die höchstrichterliche Rechtsprechung dazu neigen könnte, den modernen Juristen zunehmend zu folgen.

Rechtspolitisch richtig spannend sind Bergers Ausführungen zur Rolle der Europäischen Union (EU), die kompetenzrechtlich im Archivrecht bisher fast nichts zu melden hatte, aber über die Notwendigkeiten der Digitalisierung (Bedarf an Authentizität, Informationsdienstleistung, Standardisierung, Harmonisierung und Vertraulichkeit) das Archivrecht weit mehr beeinflusst, als es selbst Spezialisten bewusst sein dürfte. Zwar sind die EU-Kompetenzen in den Bereichen Kultur und öffentliche Verwaltung noch subsidiär gegenüber denen der Mitgliedstaaten, doch könnte gerade die DSGVO hier einen massiven Innovationsschub bringen.

Die Richtung der nötigen Innovation wird von Berger präzise und gut begründet dargetan: Wir benötigen das (historische) Verwaltungswissen als Grundlage für die Weiterentwicklung unserer Informationsgesellschaft, um deren Rationalität künftig zu sichern. Dafür müssen sich die Archive vom Image staubiger Kellerräume befreien und sich zu einer Zentralkompetenz für Informationssammlung, -speicherung und -auswertung fortentwickeln.

Ganz nebenbei liefert Berger mit seiner Analyse eine umfassende Kommentierung des aktuellen Archivrechtes mit seinen vielen landesspezifischen Abweichungen und Sonderwegen und zeigt damit zugleich auf, welche unterschiedlichen Antworten Recherchierende erhalten können, die in (Landes-) Archiven nach Informationen suchen. Dies macht den Harmonisierungsbedarf im Archivrecht deutlich, der vom Modernisierungsbedarf überlagert wird: Dieser beginnt mit der Digitalisierung analoger Unterlagen und der aktuellen Erreichbarkeit der digitalen Materialien. Die Bereitstellung darf sich nicht darauf beschränken, nur Hilfestellungen zu geben. Als Quellenexperten sind Archivare vielmehr selbst die geborenen Forschenden sowie diejenigen, die ihre Erkenntnisse populär, z.B. über Internetangebote, präsentieren sollten.

Äußerst erfreulich ist, dass sich Berger nicht nur mit der Archivierung, sondern auch mit der Archivnutzung befasst und dabei offenlegt, welche Zweckbreite von Archiven abgedeckt werden kann. Dies beginnt mit Informationsdienstleistungen für die Verwaltung, die das Archivmaterial ursprünglich liefert, bis hin zu Nutzungsformen im „öffentlichen Interesse“, von denen bisher nur wenige zur Anwendung kommen, etwa im Gesundheitsbereich, im Bereich der Personensuche, der politischen Bildung oder der (rechtlichen) Begutachtung. Dabei stellt sich zunehmend die Frage der Machbarkeit und Zulässigkeit von Massendatenauswertungen, also des Einsatzes von „Big Data“ auf der Basis des Archivmaterials.

Die Doktorarbeit von Berger ist viel mehr als eine gelungene wissenschaftliche Arbeit. Sie ist zugleich ein Leitfaden für die Politik zur Reform des Archivrechts, ein Handbuch für Archivarinnen und Archivare und für Datenschützer die zentrale Quelle zur Beantwortung von Fragen zur Wechselbeziehung zwischen Datenschutz und Archivrecht. Eine übersichtliche Gliederung, ein imposanter Quellennachweis mit einem ausführlichen Literaturverzeichnis lässt nur wenige Wünsche offen. Ein Wunsch wäre ein Stichwortverzeichnis, um das Buch noch besser als Nachschlagewerk nutzen zu können. Tatsächlich verbleiben einige Bereiche, die nicht behandelt werden: So wäre es reizvoll und erkenntnisfördernd, die konkreten Erfahrungen mit dem Stasi-Unterlagen-Archiv, das dem Bundesarchiv zugeordnet wird, mit den Ergebnissen von Berger zu spiegeln. Ein hochkontroverses Thema, das nicht behandelt wird, ist die Abgabepflicht von privaten Archiven mit Unterlagen von früheren Funktionsträgern, insbesondere aus der Politik. Und schließlich stellt sich generell die Frage nach dem Verhältnis privater Datenverarbeitung, etwa von Portalanbietern wie Google oder Facebook, die auch von öffentlichen Stellen genutzt werden, zu öffentlichen Archiven. Die Zukunft der Archive hängt nämlich letztlich davon ab, ob der Staat für sich den Anspruch entwickelt, zentraler Dienstleister für die informationelle Daseinsvorsorge zu sein. Zu wünschen wäre es. Berger gibt hierfür richtige Hinweise.



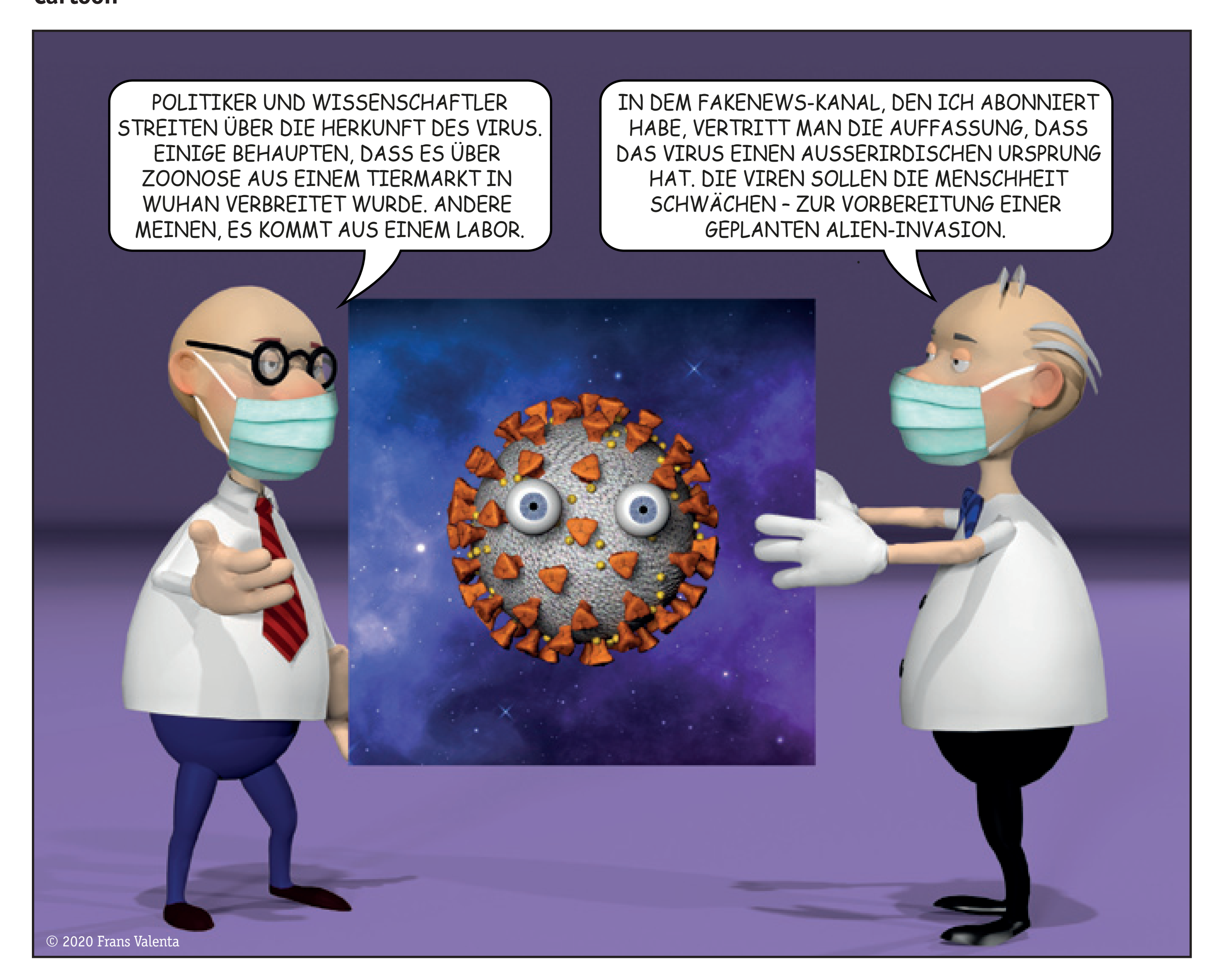
Drożdżowski, Łukasz
Datenschutzrechtliche Pflichten von Unternehmen bei der Verarbeitung genetischer Daten
Verlag Dr. Kovač, Hamburg 2019, ISBN 978-3-339-10728-2, 114 S.

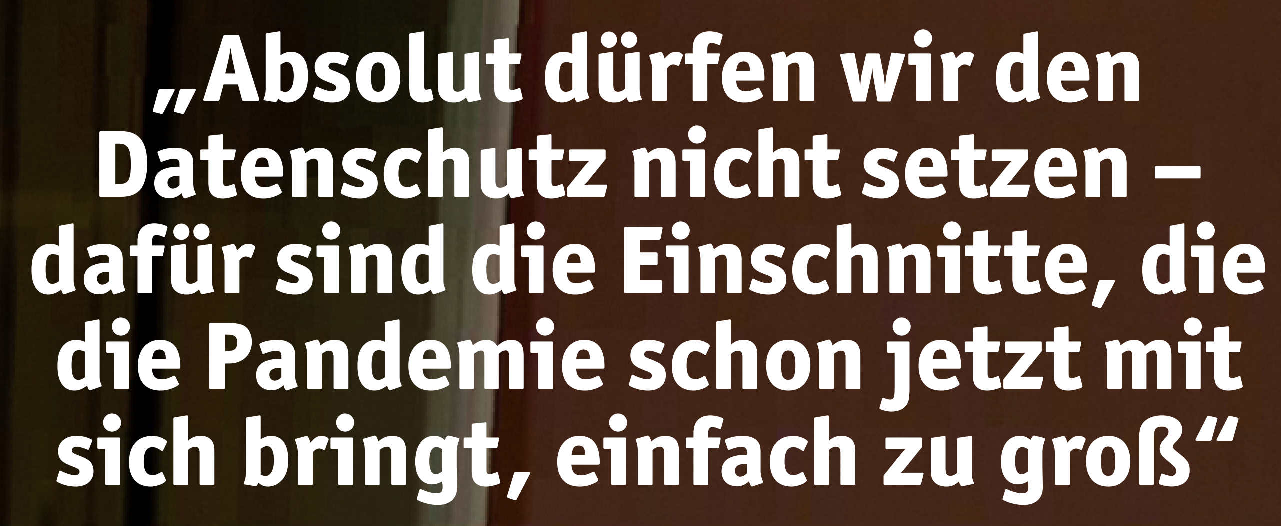
(tw) Die bereichsspezifische Behandlung von rechtlichen Fragen des Datenschutzes hat mit diesem kleinen Büchlein die Verarbeitung genetischer Daten erreicht. Diese bekommt in der Praxis eine immer größere Relevanz, insbesondere im privatwirtschaftlichen Bereich. Drożdżowski liefert nun das Material für die Anwendung der europäischen Datenschutz-Grundverordnung (DSGVO) für so wichtige Bereiche wie die Forschung, die Versicherungsbranche oder Beschäftigungsverhältnisse. Dabei geht es um die Klärung des Wechselspiels zwischen der nationalen Regulierung, insbesondere im Gendiagnostikgesetz (GenDG), und der DSGVO. Für den Bereich der Versicherungswirtschaft wird ein knapper Vergleich mit den nationalen Regelungen in Belgien, Irland, Polen, Österreich und Großbritannien vorgenommen.

Der Autor behandelt systematisch alle rechtlich relevanten Fragestellungen: von der Besonderheit genetischer Daten und ihrer persönlichkeitsrechtlichen Relevanz über die Begrifflichkeit der DS-GVO, die Anforderungen an eine einwilligungsbasierte Verarbeitung bis hin zu den Anforderungen an die Verarbeitung, jeweils unter spezifischer Bezugnahme auf die besondere Datenkategorie: Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, zudem die organisatorischen Pflichten vom Verarbeitungsverzeichnis über Melde- und Benachrichtigungspflichten, Folgenabschätzung bis hin zur Tätigkeit des Datenschutzbeauftragten.

Das Büchlein zeichnet sich durch eine saubere Quellenauswertung und -präsentation aus, so dass allein hierüber die nicht gerade üppige Literatur zu dem Thema bis zum Jahr 2018 erschlossen ist. Förderlich für die Nutzung als Handbuch sind auch die klare und detaillierte Gliederung sowie das spezifische Literaturverzeichnis und die deskriptive Behandlung der jeweiligen Themen. Eine kritische vertiefende Aufarbeitung war offenbar nicht das Ziel des Autors, sondern die Vermittlung von Wissen und Material, das ansonsten nirgends so aktuell und konzentriert zur datenschutzrechtlichen Behandlung von Gendaten verfügbar ist. Wer damit zu tun hat, dem ist das Werk sehr zu empfehlen.

Cartoon





Axel Voss (CDU) im Interview mit der FAZ

https://www.faz.net/aktuell/politik/
wer-die-corona-app-hat-soll-zuerst-wieder-ins-restaurant-duerfen-16759932.html